AMERICAN JOURNAL OF MATHEMATICS

FOUNDED BY THE JOHNS HOPKINS UNIVERSITY

PUBLISHED UNDER THE JOINT AUSPICES OF

THE JOHNS HOPKINS UNIVERSITY
AND
THE AMERICAN MATHEMATICAL SOCIETY

Volume LXXVII, Number 3
JULY, 1955

THE JOHNS HOPKINS PRESS
BALTIMORE 18, MARYLAND
U. S. A.

CONTENTS

The AMERICAN JOURNAL OF MATHEMATICS appears four times yearly.

The subscription price of the JOURNAL is $8.50 in the U. S.; $8.75 in Canada; and $9.00 in other foreign countries. The price of single numbers is $2.50.

Manuscripts intended for publication in the JOURNAL should be sent to Professor AUREL WINTNER, The Johns Hopkins University, Baltimore 18, Md.

Subscriptions to the JOURNAL and all business communications should be sent to THE JOHNS HOPKINS PRESS, BALTIMORE 18, MARYLAND, U. S. A.

Entered as second-class matter at the Baltimore, Maryland, Postoffice, acceptance for mailing at special rate of postage provided for in Section 1103, Act of October 3, 1917, Authorized on July 3, 1918.

PRINTED IN THE UNITED STATES OF AMERICA
BY J. H. FURST COMPANY, BALTIMORE, MARYLAND

ON THE FORMS OF THE PREDICATES IN THE THEORY OF CONSTRUCTIVE ORDINALS (SECOND PAPER).*

By S. C. KLEENE.

In the first paper of this title, the author presented a technique for use in attempts to reduce inductive definitions to explicit definitions, and claimed by means of it to show that the predicates $a \varepsilon O$ and $a <_o b$ of the system S_3 of notation for ordinal numbers are expressible in the respective forms $(x)(Ey)R(a,x,y)$ and $(x)(Ey)S(a,b,x,y)$ where R and S are primitive recursive predicates. To apply the technique, the inductive definition of a predicate P is first rewritten as an equivalence, and then a solution of the latter for P as an unknown predicate is sought.

A fallacy occurs in the preliminary step:[1] the equivalence does not fully express the inductive definition, but may admit other solutions for P than the predicate defined by the inductive definition. It is thus necessary to supplement the application of the technique by a proof that the particular solution obtained is not "extraneous". It appears now that this supplementary reasoning can be given for the applications of the technique in which the proposed solution has only an existential quantifier, but fails in the final application (to $a \varepsilon Q$ in **14**) where there is also a universal quantifier.

In the present paper we shall show that the result claimed in the first paper becomes correct, if a variable α for a 1-place number-theoretic function is substituted for the number variable x; i.e., $a \varepsilon O$ and $a <_o b$ are expressible in the respective forms $(\alpha)(Ey)R(a,\alpha,y)$ and $(\alpha)(Ey)S(a,b,\alpha,y)$ where R and S are primitive recursive (**29** Theorem II).[2] Conversely, every predicate

* Received December 4, 1953. The references to [13] and [15] were added June 3, 1954. The ideas for the proof of Theorems I and II were obtained in March 1950 while the author was on research leave supported by the University of Wisconsin Graduate School and held a John Simon Guggenheim Memorial Fellowship. The first paper of this title appeared in this JOURNAL, vol. 66 (1944), pp. 41-58.

[1] This is the error noted in the bibliographical references to the first paper in [10] and [11].

[2] A function or predicate with variables for 1-place number-theoretic functions as well as for natural numbers we call *primitive recursive* (as in [12]), if as a function or predicate of its number variables it is primitive recursive uniformly in its function variables in the sense of [11] p. 234. Like terminology has already been used in the case of general recursiveness in [10] pp. 681-682 and in [12].

of the form $(\alpha)(Ey)R(a,\alpha,y)$ where R is general recursive is expressible in the form $\xi(a)\,\varepsilon\,O$ where ξ is primitive recursive (**25** Theorem I). It follows by the theory of arithmetical predicates and function quantifiers[3] that $a\,\varepsilon\,O$ and $a <_o b$ are not expressible in the dual forms $(E\alpha)(y)R(a,\alpha,y)$ and $(E\alpha)(y)S(a,b,\alpha,y)$ with recursive R and S, respectively; a fortiori,[4] they are not arithmetical, so in particular the result claimed originally is false. Most of the work done in the first paper is utilized in proving the present results. We give an example of a primitive recursive linear ordering of the natural numbers which is a well-ordering with respect to the arithmetical functions but not with respect to all the number-theoretic functions (**26** (J)). Classical methods are used in this example and to some extent elsewhere. The results hold also for the relative version of the theory of constructive ordinals (in **30**).

Some of the numbering and symbolism is continued from the first paper. Sections **18** and **19** indicate in detail what can be kept and what must be rejected in that paper. Readers not having that paper at hand may begin with **20**. For their convenience, information from that paper will be repeated here as needed; and they can choose from various sources cited in the footnotes for the notations and results of the theory of recursive functions which are employed.

18. The reduction technique. On p. 46 of the first paper, we rewrote the inductive definition 1-4 as an equivalence (18), assuming uncritically that the latter is equivalent as a definition of $P(a)$ to the former.

But suppose that the formal deductive system, for which the $P(a)$ of 1-4 is the arithmetized provability predicate, includes among its symbols $\supset$ and among its rules of inference modus ponens

$$\frac{\mathrm{A},\ \mathrm{A}\supset\mathrm{B}}{\mathrm{B}}.$$

Also suppose the arithmetrization to have been carried out (as is usual) so that $A(a)$, $B(a,b)$ and $C(a,b,c)$ are each true only when a is (the Gödel number of) a formula. In this case, (18) can have as solution for $P(a)$ not only $P(a) \equiv \{a \text{ is provable}\}$, which we intended, but also $P(a) \equiv \{a \text{ is a formula}\}$. For each formula A is inferable from two other formulas, e.g., A and $\mathrm{A}\supset\mathrm{A}$, by modus ponens. Hence, when $P(a) \equiv \{a \text{ is a formula}\}$: For each a which makes the left side of (18) true, the third disjunctive

[3] [12] Theorem 3.

[4] [12] Theorem 5.

member $(Ex)(Ey)[P(x)\&P(y)\&C(a,x,y)]$ of the right side, and hence the right side itself, will be true. Conversely, for each a which makes the right side true, and hence makes either $A(a)$, or $B(a,x)$ for some x, or $C(a,x,y)$ for some x and y, true, the left side will be true.

What is lost in rewriting the inductive definition 1-4 as the equivalence (18) is part of the effect of the extremal clause 4. The predicate $P(a)$ defined by 1-4 (write it now $P_0(a)$) is that predicate $P(a)$ satisfying (18) for which the set $\hat{a}P(a)$ of the a's which make $P(a)$ true is the least. In other words, $P_0(a)$ is the solution of (18) such that, for any solution $P(a)$ of (18),

$$P_0(a) \rightarrow P(a). \tag{18.1}$$

This implication can be proved by induction, in the form which corresponds to the inductive definition 1-4 of $P_0(a)$.

In particular, then (18.1) holds when $P(a)$ is our solution

$$P(a) \equiv (Ex)R(a,x) \tag{23}$$

of (18). But also, by course-of-values induction on x (using (13)), we can show from the definition (22) of $R(a,x)$ that

$$(a)[R(a,x) \rightarrow P_0(a)], \tag{18.2}$$

whence (via $(x)(a)[R(a,x) \rightarrow P_0(a)]$ and $(a)(x)[R(a,x) \rightarrow P_0(a)]$)

$$(Ex)R(a,x) \rightarrow P_0(a). \tag{18.3}$$

So, by (18.1) (applied to $(Ex)R(a,x)$ as the $P(a)$) and (18.3), our solution $P(a) \equiv (Ex)R(a,x)$ ((23) with (22)) of (18) is in fact $P_0(a)$.

Thus with the help of the supplementary argument given now, we do establish that $\{a$ is provable$\}$ is expressible in the form $(Ex)R(a,x)$ with a primitive recursive R.

Likewise, at each place in the paper where we rewrote an inductive definition as an equivalence, we lost part of the effect of the extremal clause. But in every case where we solved that equivalence by a predicate of the form $(Ex)R(a,x)$ or $(Ex)R(a,b,x)$, we can show by induction on x that our solution is the predicate defined by the inductive definition.

19. Conclusions from the first paper. In this manner the conclusions of the first paper can be upheld, except those of **14** and **15** including Theorem 1. and (41) in **16**.[5] By **25** Corollary to Theorem I, we see now that Theorem 1

[5] On p. 43 omit the stars on (4) and (11) (cf. [11] *86 and *95 pp. 162-163). On p. 52 after (V) and (VI) the "(Use (IV).)" is unnecessary. On p. 53 in (30) and

and (41) are false. By **25** Theorem I with [12] Theorem 5, likewise Theorem IX of [9] Section 15, our "proof" of which depended on Theorem 1, is false.

20. The predicates $a \varepsilon O$ and $a <_o b$ (recapitulated).[6] In this paper we are writing $T(z,x,y)$ for $T_1(z,x,y)$, and $\Phi(z,x)$ for $\Phi_1(z,x)$ $(\cong U(\mu y T_1(z,x,y)))$.[7]

Let $0_o = 1$, $(n+1)_o = 2^{n_o}$. By saying that y defines y_n recursively as a function of n_o, we mean that $(n)\{\Phi(y,n_o)$ is defined and $= y_n\}$. The predicates $a \varepsilon O$ and $a <_o b$ of the system S_3 of notation for ordinal numbers (of the constructive first and second number classes) were introduced by the following inductive definition:[8]

$O1$. $1 \varepsilon O$. $O2$. If $y \varepsilon O$, then $2^y \varepsilon O$ and $y <_o 2^y$. $O3$. If, for each n, $y_n \varepsilon O$ and $y_n <_o y_{n+1}$, and if y defines y_n recursively as a function of n_o, then $3 \cdot 5^y \varepsilon O$ and, for each n, $y_n <_o 3 \cdot 5^y$. $O4$. If $x \varepsilon O$, $y \varepsilon O$, $z \varepsilon O$, $x <_o y$ and $y <_o z$, then $x <_o z$. $O5$. $a \varepsilon O$ and $a <_o b$ only as required by $O1$-$O4$.

We recall the following lemmas (I)-(VIII) from **12**. Here $C(b)$ is a class of numbers depending on b (defined in **12**), such that (as shown in **13**)

$$(32) \qquad a \varepsilon C(b) \equiv (Ex) V(a,b,x)$$

for a certain primitive recursive V. We write $a \leqq_o b$ for $a <_o b \vee a = b$, $a >_o b$ for $b <_o a$, etc.

(I) *If $a \varepsilon O$, then $a \neq 0$.* (II) *If $a <_o b$, then $b \neq 1$.* (III) *$C(1)$ is empty.* (IV) *If $a <_o b$, then $a \varepsilon O$ and $b \varepsilon O$.* (V) *If $a <_o 2^y$, then $a \leqq_o y$.* (VI) *If $a <_o 3 \cdot 5^y$, then, for some n, $a \leqq_o y_n$, where $y_n = \Phi(y, n_o)$.* (VII) *If $b \varepsilon O$, then $a \varepsilon C(b) \rightarrow a <_o b$.* (VIII) *If $b \varepsilon O$, then $a <_o b \rightarrow a \varepsilon C(b)$.*

---

(31) read "$b = 3 \cdot 5^y$" for "$a = 3 \cdot 5^y$". On p. 54 in (35) read "$a = 3 \cdot 5^{(a)_3}$" for "$e = 3 \cdot 5^{(a)_3}$" (an adaptation of **14** is used in **27**). In order that **16** Theorem 2 give the full force of (41)-(44), it should be added in each part that the function also map one-to-one the complement of the one set on a subset of the complement of the other; this being added, the first part becomes false. Theorem 3 (which should have been indicated as classical) is now included in the much stronger Corollary to Theorem I (also classical).

[6] The reader may wish to follow the modifications outlined in **30** for the relative version of the theory as he reads **20-29** giving the absolute version.

[7] **10**; or [9] Sections 4, 7, 10; or [11] pp. 225, 279, 281, 288, 327, 330, 340.

[8] The theory of constructive ordinals in various versions appears in Church-Kleene [4], Church [3], Kleene [8] (cf. Section 3 for n_o, Section 5 for S_3) and Turing [20] Section 7.

We add several further lemmas. Some of these are proved, as were preceding ones, by induction in a form which corresponds to the inductive definition $O1$-$O5$. This is illustrated by the proofs of (VII) in **12** and (XX) in **22**, which are given in full.

(IX) *If* $a \varepsilon O$, *then* $a \geqq_o 1$. (By induction.) (X) *If* $a \varepsilon O$, *then, for each number-theoretic function* $\alpha(n)$ *such that* $\alpha(0) = a$ *and* $(n)[\alpha(n) \neq 1 \rightarrow \alpha(n) >_o \alpha(n+1)]$, *there is a number* k *such that* $\alpha(k) = 1$. (By induction. For example in the part where it is assumed that $a = 2^y$ with $y \varepsilon O$, by (I), $a \neq 1$, so $a = \alpha(0) >_o \alpha(1)$. By (V), either $y = \alpha(1)$ (Case A) or $y >_o \alpha(1)$ (Case B). We apply the hypothesis of the induction in Case A to $\beta(n) = \alpha(n+1)$; in Case B (then by (II), $y \neq 1$) to $\beta(n) = y$ if $n = 0$, $= \alpha(n)$ if $n \neq 0$.)

(XI) *For each* a, $\overline{a <_o a}$. (By reductio ad absurdum, from (II), (IV), and (X) applied to $\alpha(n) = a$.) (XII) *If* $a <_o b$, *then* $\overline{b <_o a}$. (By (IV), $O4$ and (XI).) (XIII) If $c \varepsilon O$, $a \leqq_o c$ *and* $b \leqq_o c$, *then* $a <_o b$ *or* $a = b$ *or* $a >_o b$. (By induction on c.)

Together $O4$, (XI) and (XII) give that O is partially ordered by $<_o$. Then by (XIII) the members of O which are $<_o$ a given member b are linearly ordered, and indeed by (X) with (II) well-ordered, by $<_o$. Thus far we have not had to mention the classical second number class.

Letting $|1| = 0$, $|2^y| = |y| + 1$ for $y \varepsilon O$, and $|3 \cdot 5^y| = \lim_n |y_n|$ for $3 \cdot 5^y \varepsilon O$ and $y_n = \Phi(y, n_O)$, each member b of O represents an ordinal $|b|$ of the first or second number class, in such a manner that whenever $a <_o b$ then $|a| < |b|$ and that for each $\alpha < |b|$ there is a member a of O such that $|a| = \alpha$ and $a <_o b$.[9] By this with (XIII), the ordering of the set $\hat{a}(a <_o b)$ by $<_o$ is of the type $|b|$. The least ordinal $> |b|$ for every $b \varepsilon O$ is called ω_1.

21. A digression concerning recursive well-orderings. A partial recursive function $\mathrm{enm}(b, m)$ which for each fixed $b >_o 1$ enumerates the numbers $<_o b$ is constructible by the method used in the earliest version of the theory.[10] However it is worth noting that the result is immediate from **12** and **13**. It is easily arranged that enm be primitive recursive and that the enumeration be without reptitions when b represents an infinite ordinal. In detail:

---

[9] Cf. **11**, [3], [8], and for an earlier version [4]. Also for (XIII), cf. [3] pp. 229-230.

[10] [4] p. 20 enm, and [8] p. 154 end Section 3. Also cf. [20] pp. 188-189 Inf.

Combining (VII) and (VIII) with (32),

$$(21.1) \qquad b \varepsilon O \rightarrow (a <_o b \equiv (Ex) V(a, b, x)).$$

Let $\mathrm{Fin}(b) \equiv (En)_{n<b}[b = n_o]$, so $\mathrm{Fin}(b) \equiv \{b \varepsilon O$ by $O1$ and $O2$ only$\} \equiv \{b$ represents a finite ordinal$\}$. Let $\mathrm{nat}(b) = \mu n_{n<b}[b = n_o]$, so that $\mathrm{nat}(n_o) = n$. (When $\mathrm{Fin}(b)$, $\mathrm{nat}(b)$ is $|\, b \,|$ as a natural number.) We use $(x)_i$ in the sense of [11].[11] Now in the case $\overline{\mathrm{Fin}}(b)$ (whether or not $b \varepsilon O$), let $\mathrm{enm}(b, m)$ be $(m)_0$, if $V((m)_0, b, (m)_1)$ and $(m)_0$ is not among $\mathrm{enm}(b, 0), \cdots, \mathrm{enm}(b, m-1)$, and otherwise let $\mathrm{enm}(b, m)$ be the first among $0_o, \cdots, m_o$ which is not among $\mathrm{enm}(b, 0), \cdots, \mathrm{enm}(b, m-1)$. In the case $\mathrm{Fin}(b)$, let $\mathrm{enm}(b, m) = (\mathrm{nat}(b) \dot{-} (m+1))_o$.[12] This gives a course-of-values recursion on m for $\mathrm{enm}(b, m)$, so enm is primitive recursive.[13]

(XIV) *If* $b \varepsilon O$ *and* $\overline{\mathrm{Fin}}(b)$, *then* $(n)[n_o <_o b]$. (By induction.) (XV) *There is a primitive recursive function* $\mathrm{enm}(b, m)$ *such that*: (i) *If* $b = n_o$, *then* $\mathrm{enm}(b, m) = (n \dot{-} (m+1))_o$. (ii) *If* $b \varepsilon O$ *and* $\overline{\mathrm{Fin}}(b)$, *then* $\mathrm{enm}(b, 0)$, $\mathrm{enm}(b, 1)$, $\mathrm{enm}(b, 2), \cdots$ *is an enumeration without repetitions of* $\hat{a}(a <_o b)$.

In Cantor's theory, ordinals arise on the one hand as the order types of well-ordered sets, and on the other as the objects generated by certain principles. In the present theory of constructive ordinals, it is the latter version of the theory which is made constructive. We inquire now into the relation between this and the result of making the first version constructive, i. e., of requiring the well-ordering to be recursive.

(A) *There is a partial recursive ternary relation* $m <_b n$ *such that, for each fixed* b: *If* $b \varepsilon O$ *and* $\overline{\mathrm{Fin}}(b)$, *then the binary relation* $m <_b n$ *is a general recursive well-ordering of the natural numbers of order type* $|\, b \,|$.[14]

Proof. Suppose $b \varepsilon O$ and $\overline{\mathrm{Fin}}(b)$. The numbers $<_o b$ are well-ordered by $<_o$ with the order type $|\, b \,|$ (end **20**). But $\mathrm{enm}(b, 0), \mathrm{enm}(b, 1), \mathrm{enm}(b, 2), \cdots$ is an enumeration of them without repetitions. So it will suffice to define

[11] [11] p. 230, viz., $(x)_i = \{$the number of times x contains the $i+1$-st prime number as factor$\}$ if $x \neq 0$, $= 0$ if $x = 0$. The author originally introduced $(x)_1, \cdots, (x)_m$ in [9] (1943) p. 50 for an unspecified m-tuple of functions with certain properties, and then in the first paper of this title (1944) **5** defined $(x)_i$ so that the $(x)_{i+1}$ there is the $(x)_i$ now; but since 1946 he has undertaken to standardize the notation $(x)_i$ in its present meaning (e. g., it was so used at his suggestion in Nelson's [16] (1947)).

[12] $n \dot{-} m = n - m$ if $n \geqq m$, $= 0$ otherwise (cf. [11] p. 223 #6).

[13] Péter [17] Section 1 or [18] Section 3, Kleene [11] Section 46.

[14] A related result is given by Turing [20] p. 183 (vi).

$m <_b n$ partial recursively so that, for the b in question, $m <_b n \equiv \text{enm}(b, m) <_o \text{enm}(b, n)$. To determine whether $\text{enm}(b, m) <_o \text{enm}(b, n)$, we first check that $m \neq n$. If $m \neq n$, then either $\text{enm}(b, m)$ occurs in the enumeration $\text{enm}(\text{enm}(b, n), 0), \text{enm}(\text{enm}(b, n), 1), \text{enm}(\text{enm}(b, n), 2), \cdots$, which happens if $\text{enm}(b, m) <_o \text{enm}(b, n)$ and only then (since $\text{enm}(b, m) = \text{enm}(b, n) = 1$ is excluded), or else $\text{enm}(b, n)$ occurs in the enumeration $\text{enm}(\text{enm}(b, m), 0)$, $\text{enm}(\text{enm}(b, m), 1), \text{enm}(\text{enm}(b, m), 2), \cdots$, which happens if and only if $\text{enm}(b, m) >_o \text{enm}(b, n)$. So we take

$$m <_b n \cong m \neq n \,\&\, \text{enm}(\text{enm}(b, n), T) = \text{enm}(b, m)$$

where

$$T \cong \mu t[\text{enm}(\text{enm}(b, n), t) = \text{enm}(b, m) \vee \text{enm}(\text{enm}(b, m), t) = \text{enm}(b, n)].$$

(B) *To any general recursive well-ordering of the natural numbers, there is a primitive recursive well-ordering of the natural numbers with the same order type.*[15]

Proof. The construction which follows will lead from a given general recursive well-ordering $\prec$ of order type α to a primitive recursive one $\prec'$ of type $\omega + \alpha$. But for $\alpha \geqq \omega^2$, $\omega + \alpha = \alpha$; and for $\alpha < \omega^2$, a primitive recursive well-ordering of type α is easily defined.

Let e be a Gödel number of (or define recursively) the general recursive ordering predicate $m \prec n$; so $(m)(n)(E!x)T_2(e, m, n, x)$ and

$$T_2(e, m, n, x) \to [m \prec n \equiv U(x) = 0].^{16}$$

For any natural number n, let the *image of* n be $2^n \cdot 3^{\max_{m \leqq n} \mu x T_2(e, m, n, x)}$. If l is the image of some number (in symbols, $\text{Im}(l)$), that number is $(l)_0$. In the new well-ordering $\prec'$, the non-images in order of magnitude among themselves shall precede the images ordered among themselves as the numbers of which they are images were ordered in the original ordering $\prec$. Since the class of the non-images is infinite, the new ordering $\prec'$ is of order type $\omega + \alpha$. The following formulas show that the new ordering $\prec'$ is primitive recursive.

$$\text{Im}(l) \equiv l = 2^{(l)_0} \cdot 3^{(l)_1} \,\&\, (Em)_{m \leqq (l)_0} T_2(e, m, (l)_0, (l)_1)$$
$$\&\, (m)_{m \leqq (l)_0} (Ex)_{x \leqq (l)_1} T_2(e, m, (l)_0, x),$$

---

[15] By [11] pp. 285-287 Example 1, 'primitive recursive' can be strengthened here to 'elementary' in the sense of P. Csillag and L. Kalmár (cf. [6], [18] Section 8, or [11] p. 285).

[16] [9] pp. 52-53 Theorem IV, [11] p. 288 Theorem IX, or (briefly) **10.** "$(E!x)$" means "there exists a unique x such that".

$$k \prec' l \equiv \{\mathrm{Im}(k) \,\&\, \overline{\mathrm{Im}}(l) \,\&\, k < l\} \vee \{\overline{\mathrm{Im}}(k) \,\&\, \mathrm{Im}(l)\}$$
$$\vee \{\mathrm{Im}(k) \,\&\, \mathrm{Im}(l) \,\&\, \{[(k)_0 < (l)_0 \,\&\, U(\mu x_{x<l} T_2(e, (k)_0, (l)_0, x)) = 0]$$
$$\vee [(k)_0 > (l)_0 \,\&\, U(\mu x_{x<k} T_2(e, (l)_0, (k)_0, x)) \neq 0]\}\}.$$

(C) *There is a primitive recursive ternary relation $m <_b' n$ such that, for each fixed b: If $b \in O$ and $\overline{\mathrm{Fin}}(b)$, then the binary relation $m <_b' n$ is a primitive recursive well-ordering of the natural numbers of order type $|b|$.*

Proof. We apply the method of proof of (B) to the $m <_b n$ of (A) as the $m \prec n$. But now we can distinguish primitive recursively which elements in the given ordering are infinite; namely $\{n \text{ is infinite}\} \equiv \overline{\mathrm{Fin}}(\mathrm{enm}(b, n))$. So by letting all numbers not images of infinite elements precede the images only of infinite elements, we avoid the increase for $\alpha < \omega^2$ from α to $\omega + \alpha$. As a Gödel number e of the ordering $m <_b n$, we have $S_2^1(d, b)$,[17] where d is a Gödel number of $m <_b n$ as predicate of b, m, n.

By (A), the order types of general (and hence by (B), or directly by (C), of primitive) recursive well-orderings of the natural numbers include all transfinite ordinals $< \omega_1$. That they include only such ordinals was shown by Markwald [15] (and independently by Clifford Spector, from whom the author first learned the result in February 1954 shortly before [15] was received in Madison).

22. Sums of ordinal notations. The addition of ordinal notations was treated briefly by Church and Kleene.[18] We redo the treatment, in order to secure an additional property of the sum function which we shall need now ((XX) below).

We seek a recursive function $a +_o b$ such that

$$(22.1) \qquad a +_o b \cong \begin{cases} a \text{ if } b = 1 \,\&\, a \neq 0 \quad \text{(Case 1)}, \\ 2^{a +_o y} \text{ if } b = 2^y \text{ where } y \neq 0 \quad \text{(Case 2)}, \\ 3 \cdot 5^{d_{a,y}} \text{ if } b = 3 \cdot 5^y \quad \text{(Case 3)}, \\ 7 \text{ otherwise} \quad \text{(Case 4)}, \end{cases}$$

where (in Case 3) $d_{a,y}$ defines recursively $a +_o \Phi(y, n_0)$ as a function of n_0.[19] We obtain such a function $a +_o b$ as follows. Let

$$\theta(z, a, y, n) \cong \Phi_2(z, a, \Phi(y, n)).^7$$

---

[17] **End 10**, or [8] p. 153, or [11] p. 342 Theorem XXIII.[25]

[18] [4] p. 18, [8] p. 154. Also Turing [20] p. 188.

[19] Here, since $a +_o \Phi(y, n_0)$ may be undefined, we mean that $(n)\{\Phi(d_{a,y}, n_0) \cong a +_o \Phi(y, n_0)\}$.

Let p define $\theta(z, a, y, n)$ recursively.[16] Let[11,17]

$$\begin{aligned}\psi(z,a,b) \cong \mu t[&\{b = 1 \,\&\, a \neq 0 \,\&\, t = a\}\\ &\vee \{b = 2^{(b)_0} \,\&\, (b)_0 \neq 0 \,\&\, t = 2^{\Phi_2(z,a,(b)_0)}\}\\ &\vee \{b = 3 \cdot 5^{(b)_2} \,\&\, t = 3 \cdot 5^{S_1^3(p,z,a,(b)_2)}\}\\ &\vee \{(b \neq 1 \vee a = 0) \,\&\, (b \neq 2^{(b)_0} \vee (b)_0 = 0) \,\&\, b \neq 3 \cdot 5^{(b)_2} \,\&\, t = 7\}].\end{aligned} \tag{22.2}$$

By the recursion theorem,[20] there is a number e which defines $\psi(e, a, b)$ recursively. Let $a +_o b \cong \psi(e, a, b)$. This gives $a +_o b$ as a partial recursive function, but in fact it is primitive recursive.[21]

(XVI) *If* $a \varepsilon O$ *and* $b \varepsilon O$, *then* (a) $a +_o b \varepsilon O$ *and* (b)

$$(c)[c <_o b \to a +_o c <_o a +_o b].$$

The proof is by induction on b with a fixed. Parts 1 and 2 (for $b \varepsilon O$ by $O1$ and $O2$, respectively) are straightforward. For 3, assume that $b = 3 \cdot 5^y$ where y is as in $O3$, and as hypothesis of the induction that (XVI) applies to each y_n as the b. (a) By Case 3 of (22.1), $a +_o b = 3 \cdot 5^d$ where for each n, $\Phi(d, n_O)$ is defined (call it d_n) and $d_n = a +_o y_n$. Applying the hypothesis of the induction, we have by (a) (for y_n as the b) $d_n \varepsilon O$ and by (b) (for y_n, y_{n+1} as the c, b) $d_n <_o d_{n+1}$. Hence by $O3$, $3 \cdot 5^d \varepsilon O$ and $d_n <_o 3 \cdot 5^d$, i.e., $a +_o b \varepsilon O$ and $a +_o y_n <_o a +_o b$. (b) Assume $c <_o b$. By (VI), for some n, either $c = y_n$ (Case A) or $c <_o y_n$ (Case B). Case A. $a +_o c = a +_o y_n <_o a +_o b$. Case B. By the hypothesis of the induction (applied to c, y_n as the c, b), $a +_o c <_o a +_o y_n$. But $a +_o y_n <_o a +_o b$. By $O4$, $a +_o c <_o a +_o b$.

(XVII) *If* $a \varepsilon O$ *and* $b >_o 1$, *then* $a +_o b >_o a$. (Use (IV), (XVI) (b), (I), (22.1).) (XVIII) *If* $a \varepsilon O$, *then* $a +_o 1_o >_o 1$. (By (22.1), (I), $O2$ and (IX).) (XIX) *If* $a \varepsilon O$ *and* $b \varepsilon O$, *then* $a +_o b \geqq_o a$. (Use (IX), (XVII), (22.1) and (I).)

(XX) *If* $a +_o b \varepsilon O$, *then* $a \varepsilon O$ *and* $b \varepsilon O$. *In fact, for every* c *which* εO: (a) *If* $a +_o b = c$, *then* $a \varepsilon O$ *and* $b \varepsilon O$. (b) *If* $a +_o b_1 = a +_o b_2 = c$, *then* $b_1 = b_2$. (c) *If* $b \neq 1 \,\&\, a \leqq_o f <_o a +_o b = c$, *then*

$$(Eg)[g <_o b \,\&\, f = a +_o g].$$

Proof is by induction on c, as follows.

---

[20] [8] p. 153 the last result of Section 2, or [11] p. 352 Theorem XXVII.

[21] For upon using the resulting value $S_1^3(p, e, a, y)$ of $d_{a,y}$ in (22.1), we have a course-of-values recursion for $a +_o b$.[13]

1. Assume that $c = 1$. (a) Assume $a +_o b = c$. Now Cases 3 and 4 of (22.1) are excluded. Also Case 2 is excluded, since this could only apply if $a +_o y = 0$, and in none of the cases of (22.1) (for y as the b) can $a +_o y = 0$. So Case 1 applies, with $a = b = 1$. But $1 \varepsilon O$. So $a, b \varepsilon O$. (b) Assume $a +_o b_1 = a +_o b_2 = c$. By (a) applied to $a + b_1$ and $a + b_2$, $a = b_1 = b_2 = 1$. So $b_1 = b_2$. (c) By (II), $f <_o a +_o b = c$ cannot hold when $c = 1$.

2. Assume that $c = 2^d$ where $d \varepsilon O$, and as hypothesis of the induction that (XX) applies to d as the c. By $O2$, $d <_o c$. (a) Assume $a +_o b = c$. Now only Case 1 or Case 2 of (22.1) can apply. In Case 1, $a = c$ and $b = 1$. But $c, 1 \varepsilon O$. So $a, b \varepsilon O$. In Case 2, $d = a +_o y$ and $b = 2^y$. By (a) of the hypothesis of the induction, then $a, y \varepsilon O$, so using $O2$, $a, b \varepsilon O$ (and $y <_o b$). (b) Assume $a +_o b_1 = a +_o b_2 = c$. If Case 1 applies to both $a +_o b_1$ and $a +_o b_2$, we have $b_1 = b_2 = 1$. If Case 2 applied to $a +_o b_1$ but Case 1 to $a +_o b_2$, we would have $b_1 = 2^y$ where $y \neq 0$ so $b_1 \neq 1$ (and by (a) $a, b_1 \varepsilon O$, and by (IX) $b_1 >_o 1$), but $a = c$. Thus we would have $a = c = a +_o b_1 >_o a$ (by (XVII)), contradicting (XI). So this pair of cases cannot apply; and similarly vice versa. If Case 2 applies to both $a +_o b_1$ and $a +_o b_2$, we have $b_1 = 2^{y_1}$, $b_2 = 2^{y_2}$ and $c = 2^d = 2^{a +_o y_1} = 2^{a +_o y_2}$, whence $d = a +_o y_1 = a +_o y_2$. By the hypothesis of the induction, $y_1 = y_2$. So $b_1 = b_2$. (c) Assume $b \neq 1 \,\&\, a \leqq_o f <_o a +_o b = c$. Since $b \neq 1$, Case 1 does not apply to $a +_o b$; and by Case 2, $d = a +_o y$ and $b = 2^y$, whence using (a) $y \varepsilon O$ and $y <_o b$. Now by (V), either $f = d$ (Case A) or $f <_o d$ (Case B). In Case A, y is a g. In Case B, $y \neq 1$, as otherwise we would have $f <_o a +_o 1 = a$ (since by (a) $a \varepsilon O$, so by (I) $a \neq 0$), contradicting the hypothesis $a \leqq_o f$ (by (XI), (XII)). By the hypothesis of the induction there is an h such that $h <_o y \,\&\, f = a +_o h$. By $O4$ (since $y <_o b$), $h <_o b$. Thus h is a g.

3. Assume that $c = 3 \cdot 5^d$, where, for each n, $\Phi(d, n_0)$ is defined (call it d_n), $d_n \varepsilon O$ and $d_n <_o d_{n+1}$, and as hypothesis of the induction that (XX) applies to each d_n as the c. By $O3$, $d_n <_o c$. (a) Assume $a +_o b = c$. Only Case 1 or 3 of (22.1) can apply. In Case 1, $a = c$ and $b = 1$, so $a, b \varepsilon O$. In Case 3, $b = 3 \cdot 5^y$ and, for each n, $\Phi(d, n_0) \cong a +_o \Phi(y, n_0)$. But since $\Phi(d, n_0)$ is defined $(= d_n)$, $a +_o \Phi(y, n_0)$ and hence $\Phi(y, n_0)$ is defined (call it y_n),[22] so that $d_n = a +_o y_n$. By (a) of the hypothesis of the induction, $a, y_n \varepsilon O$. By (XIX), $a \leqq_o d_n$. Were $y_{n+1} = 1$, we would have $d_{n+1} = a \leqq_o d_n$,

[22] Under the weak sense ([8] p. 152 ll. 20-22, or [11] p. 327), $a +_o \Phi(y, n_0)$ can be defined only when $\Phi(y, n_0)$ is defined.

contradicting $d_n <_o d_{n+1}$. Thus $y_{n+1} \neq 1$. Also $d_n <_o d_{n+1} = a +_o y_{n+1}$. Using the hypothesis of the induction to apply (c) (with d_n, d_{n+1}, y_{n+1} as the f, c, b), there is a g such that $g <_o y_{n+1} \,\&\, d_n = a +_o g$. But $d_n = a +_o y_n$. Using the hypothesis of the induction to apply (b) (with d_n as the c), $g = y_n$. Hence $y_n <_o y_{n+1}$. Now by $O3$ we can conclude that $3 \cdot 5^y \varepsilon O$ (and for each n, $y_n <_o 3 \cdot 5^y = b$). Thus $a, b \varepsilon O$. (b) Assume $a +_o b_1 = a +_o b_2 = c$. If Case 1 applies to both $a +_o b_1$ and $a +_o b_2$, or Case 3 to either and Case 1 to the other, we can argue as under Part 2. If Case 3 applies to both, then $b_1 = 3 \cdot 5^{y_1}$ and $b_2 = 3 \cdot 5^{y_2}$ for some numbers y_1 $(= (b_1)_2)$ and y_2 $(= (b_2)_2)$, and by the actual construction of the function $+_o$, $a +_o b_1 = 3 \cdot 5^{S_1^3(p,e,a,(b_1)_2)}$ and $a +_o b_2 = 3 \cdot 5^{S_1^3(p,e,a,(b_2)_2)}$. Hence $S_1^3(p, e, a, (b_1)_2) = S_1^3(p, e, a, (b_2)_2)$. By the construction of the function $S_n^m(z, y_1, \cdots, y_m)$,[23] now $(b_1)_2 = (b_2)_2$, i.e., $y_1 = y_2$, so $b_1 = b_2$. (c) Assume $b \neq 1 \,\&\, a \leqq_o f <_o a +_o b = c$. Case 1 does not apply; and by Case 3, $b = 3 \cdot 5^y$ etc. (cf. under (a)). By (VI), for some n, either $f = d_n$ (Case A) or $f <_o d_n$ (Case B). The proof that there is a g is completed in the same manner as in Part 2.

23. Finite sums. For any number-theoretic function $\psi(x)$, let

$$(23.1) \qquad \begin{cases} \sum_{x<0}{}_o \psi(x) = 1, \\ \sum_{x<m+1}{}_o \psi(x) = \sum_{x<m}{}_o \psi(x) +_o \psi(m). \end{cases}$$

Then $\sum_{x<m}{}_o \psi(x)$ is a function of m primitive recursive in ψ. Similarly with $\psi(x, a_1, \cdots, a_n)$ instead of $\psi(x)$.

(XXI) *If* $(x)_{x<m}[\psi(x) \varepsilon O]$, *then* $\sum_{x<m}{}_o \psi(x) \varepsilon O$. (By induction on m, using (XVI) (a).) Conversely: (XXII) *If* $\sum_{x<m}{}_o \psi(x) \varepsilon O$, *then* $(x)_{x<m}[\psi(x) \varepsilon O]$. (Similarly, using (XX).) (XXIII) *If* $(x)_{x<m}[\psi(x) \varepsilon O]$ *and* $\psi(m) >_o 1$, *then* $\sum_{x<m}{}_o \psi(x) <_o \sum_{x<m+1}{}_o \psi(x)$. (Use (XVII) and (XXI).)

24. Securability. We can *represent* a finite sequence $\alpha(0), \cdots, \alpha(x-1)$ of x numbers $(x \geqq 0)$ by the single number $\bar{\alpha}(x) = \prod_{i<x} p_i^{\alpha(i)+1}$.[24] There is a particular primitive recursive predicate $T_1^1(v, z, a)$ such that, for each general recursive predicate $R(a, \alpha, x)$,[2] there is a number f such that

[23] [11] p. 342. Erratum (1952 printing): l. 7 from below, replace "$d_* \cdot \cdots$" by "$d_*[2 \exp \cdot \cdots]$".

[24] As in [10] p. 680 and [12] Footnote 2; p_i = {the $i+1$-st prime number} ([11] p. 230 #18).

$(Ex)R(a,\alpha,x) \equiv (Ex)T_1^1(\bar{\alpha}(x),f,a)$.[25] Thus any predicate of the form $(Ex)R(a,\alpha,x)$ with R general recursive can be taken to be of the form $(Ex)R(a,\bar{\alpha}(x))$ with R primitive recursive.

Define $\mathrm{Seq}(w) \equiv w \neq 0 \,\&\, (i)_{i<\mathrm{lh}(w)}[(w)_i \neq 0]$,[25] so $\mathrm{Seq}(w)$ is primitive recursive and $\mathrm{Seq}(w) \equiv \{w = \bar{\gamma}(x)$ for some γ and $x\} \equiv \{w$ represents a finite sequence $\gamma(0),\cdots,\gamma(x-1)\}$. Here $\gamma(i) = (w)_i \dot{-} 1$ $(i = 0,\cdots, x-1)$.

Consider any predicate $R(a,v)$ and any such number $w = \bar{\gamma}(x)$.

We say w (or the x-tuple $\gamma(0),\cdots,\gamma(x-1)$ which w represents) is *secured* (with respect to R and a), if $(Et)_{t\leq x}R(a,\bar{\gamma}(t))$.

We say w (or $\gamma(0),\cdots,\gamma(x-1)$) is *immediately secured* (with respect to R and a), if $\gamma(0),\cdots,\gamma(x-1)$ but no proper initial segment of it is secured, i.e., if $R(a,\bar{\gamma}(x)) \,\&\, (t)_{t<x}\bar{R}(a,\bar{\gamma}(t))$.

We say w (or $\gamma(0),\cdots,\gamma(x-1)$) is *past secured* (with respect to R and a), if w is secured but not immediately so, i.e., if $(Et)_{t<x}R(a,\bar{\gamma}(t))$.

We say w (or $\gamma(0),\cdots,\gamma(x-1)$) is *securable* (with respect to R and a), if w is secured or $(\alpha)(Et)R(a,w*\bar{\alpha}(t))$, i.e., if no matter how $\gamma(0),\cdots,\gamma(x-1)$ (if it is not already secured) is extended as $\gamma(0),\cdots,\gamma(x-1),\alpha(0),\alpha(1),\cdots$, a sequence $\gamma(0),\cdots,\gamma(x-1),\alpha(0),\cdots,\alpha(t-1)$ will eventually result which is secured.[26]

Applying this notion to the case $w = 1 = \bar{\gamma}(0)$, $(\alpha)(Ex)R(a,\bar{\alpha}(x)) \equiv \{1$ is securable with respect to R and $a\}$.

Any number w not of the form $\bar{\gamma}(x)$, i.e., such that $\mathrm{Seq}(w)$, we take to be not secured, immediately secured, past secured or securable.

Now let "securable$_E$" express the notion of securability as just defined explicitly, and "securable$_I$" the notion we define next by an inductive definition $S1$-$S3$. For brevity we are omitting the words "with respect to R and a".

$S1$. If w is secured, then w is *securable*. $S2$. If $\mathrm{Seq}(w)$, and w is not secured,[27] but, for every natural number s, $w*2^{s+1}$ is *securable*, then w is *securable*. $S3$. w is *securable* only as required by $S1$-$S2$.

(D) *If w is securable$_I$, then w is securable$_E$.*

---

[25] From [11] Theorem IV* pp. 281, 292 (with pp. 231, 291, where $\bar{\alpha}(x)$ and $T_1^1(v,z,a,x)$ are defined) by putting

$$T_1^1(v,z,a) \equiv T_1^1(\Pi_{i<\mathrm{lh}(v)}p_i^{\exp(v)_i \dot{-} 1},z,a,\mathrm{lh}(v)),$$

noting that $\mathrm{lh}(\bar{\alpha}(x)) = x$ p. 230 #20 (as in [10], or [12] Footnote 2).[11,12,24]

[26] $w*\bar{\alpha}(t)$ represents the latter sequence; cf. [11] p. 230 #21.

[27] We could omit "w is not secured" in $S2$, but we prefer to keep it, so that the inductive definition analyzes securability into two exclusive cases $S1$ and $S2$.

This is easily proved by induction in the form corresponding to the inductive definition $S1$-$S3$. Conversely:

(E) *If w is securable$_{\mathrm{E}}$, then w is securable$_{\mathrm{I}}$.*

We establish this classically. Brouwer argues (in substance) that it is the case intuitionistically (in [2] Footnote 7).

Suppose that $\mathrm{Seq}(w)$ but w is not securable$_{\mathrm{I}}$. Then by $S1$, w is not secured (so $\bar{R}(a, w*\bar{\alpha}(0))$), and by $S2$ for some number s_0, $w*2^{s_0+1}$ is not securable$_{\mathrm{I}}$ (put $\alpha(0) = s_0$, so $2^{s_0+1} = \bar{\alpha}(1)$). Then by $S1$, $w*\bar{\alpha}(1)$ is not secured (so $\bar{R}(a, w*\bar{\alpha}(1))$), and by $S2$ for some number s_1, $w*\bar{\alpha}(1)*2^{s_1+1}$ is not securable$_{\mathrm{I}}$ (put $\alpha(1) = s_1$, so $\bar{\alpha}(1)*2^{s_1+1} = \bar{\alpha}(2)$). Then by $S1$, $w*\bar{\alpha}(2)$ is not secured (so $\bar{R}(a, w*\bar{\alpha}(2))$), etc. Thus we obtain a function α such that $(t)\bar{R}(a, w*\bar{\alpha}(t))$. Hence $(\overline{\alpha})(Et)R(a, w*\bar{\alpha}(t))$, besides which w is not secured, i. e., w is not securable$_{\mathrm{E}}$.

The remarks in this section apply similarly with $a_1, \cdots, a_n$ for any fixed $n \geqq 0$ in place of a (then T_1^1 becomes T_n^1).

25. Classification of $a \in O$ and $a <_o b$ from below.

THEOREM I. *Given any general recursive predicate $R(a, \alpha, x)$, a primitive recursive function $\xi(a)$ can be found such that $(\alpha)(Ex)R(a, \alpha, x) \equiv \xi(a) \in O$.*[28]

Proof. By **24**, after choosing a primitive recursive $R(a, v)$ so that $(Ex)R(a, \alpha, x) \equiv (Ex)R(a, \bar{\alpha}(x))$, it will suffice to choose ξ so that $\xi(a) \in O$ if and only if 1 is securable with respect to this R and a. We begin by defining $\xi(a, w)$ so that $\xi(a, w) \in O$ if and only if w is securable with respect to R and a. Then we can take $\xi(a) = \xi(a, 1)$.

We choose the function $\xi(a, w)$ to satisfy

$$(25.1) \qquad \xi(a, w) = \begin{cases} 0 \text{ if } \overline{\mathrm{Seq}}(w) \text{ (Case 0)}, \\ 1 \text{ if } w \text{ is secured (Case 1)}, \\ 3 \cdot 5^{f_{a,w}} \text{ if } \mathrm{Seq}(w) \text{ but } w \text{ is not secured (Case 2)}, \end{cases}$$

where (in Case 2) $f_{a,w}$ defines recursively $\sum_{s<n}{}_o (\xi(a, w*2^{s+1}) +_o 1_o)$ as a function of n_o.

---

[28] Our proof of the implication $\xi(a) \in O \rightarrow (\alpha)(Ex)R(a, \alpha, x)$ makes use of the classical second number class.—Putting $\xi_1(a) = \xi(a) +_o a_o$, ξ_1 has the properties of ξ in the theorem, and $a \neq b \rightarrow \xi_1(a) \neq \xi_1(b)$; so the decision problem for $\hat{a}(\alpha)(Ex)R(a, \alpha, x)$ is 1-1 reducible (Post) to that for O (cf. [19], [11] p. 343 Example 2).

We obtain such a function ξ as follows. Let

$$\theta(z,a,w,b) \cong \sum_{s<\mathrm{nat}(b)}{}_O\ (\Phi_2(z,a,w*2^{s+1}) +_o 1_o)$$

(cf. **21**). Let p define θ recursively. Let

$$(25.2)\quad \psi(z,a,w) = \begin{cases} 0 \text{ if } \overline{\mathrm{Seq}}(w), \\ 1 \text{ if } \mathrm{Seq}(w) \,\&\, (Et)_{t\leq \mathrm{lh}(w)} R(a, \prod_{i<t} p_i^{(w)_i}), \\ 3\cdot 5^{S_1^3(p,z,a,w)} \text{ if } \mathrm{Seq}(w) \,\&\, (\overline{Et})_{t\leq \mathrm{lh}(w)} R(a, \prod_{i<t} p_i^{(w)_i}). \end{cases}$$

Then ψ is primitive recursive. Choose e by the recursion theorem so that e defines $\psi(e,a,w)$ recursively.[20] Let $\xi(a,w) = \psi(e,a,w)$.

Now we prove by an induction of form corresponding to the inductive definition $S1$-$S3$ of securability that, if w is securable, then $\xi(a,w)\,\varepsilon\, O$.

1. Assume w is secured. Then by Case 1 of (25.1), $\xi(a,w) = 1$. So by $O1$, $\xi(a,w)\,\varepsilon\, O$.

2. Suppose $\mathrm{Seq}(w)$, w is not secured, but, for every s, $w*2^{s+1}$ is securable, and as hypothesis of the induction that, for every s, $\xi(a,w*2^{s+1})\,\varepsilon\, O$. Then by (XVI) and (XXI), for each n, $\sum_{s<n}{}_O\ (\xi(a,w*2^{s+1}) +_o 1_o)\,\varepsilon\, O$. Moreover by (XXIII) and (XVIII), for each n,

$$\sum_{s<n}{}_O\ (\xi(a,w*2^{s+1}) +_o 1_o) <_o \sum_{s<n+1}{}_O\ (\xi(a,w*2^{s+1}) +_o 1_o).$$

Hence by (25.1) Case 2 with $O3$, $\xi(a,w)\,\varepsilon\, O$.

Conversely, we prove that, if $\xi(a,w) = c$ and $c\,\varepsilon\, O$, then w is securable. We give the proof by transfinite induction on $|\,c\,|$.[29] The cases in the proof correspond to the clauses $O1$-$O3$ by which c can $\varepsilon\, O$.

1. Assume $c = 1$. Then $\xi(a,w) = 1$; it is Case 1 of (25.1) which applies to $\xi(a,w)$; and so w is secured, a fortiori securable.

2. Assume $c = 2^y$ where $y\,\varepsilon\, O$, so by (I), $y \neq 0$. But then $\xi(a,w) = c$ is impossible under (25.1).

---

[29] Several attempts to get by with induction on c instead of on $|\,c\,|$ were unsuccessful. A difficulty is that $a +_o b$ is not necessarily $\geqq_o b$. Indeed there is no function $\circ$ such that, for all $a, b\,\varepsilon\, O$, both $a \circ b \geqq_o a$ and $a \circ b \geqq_o b$. For if e and f define recursively n_o and $(n+1)_o$, respectively, as functions of n_o, and $a = 3\cdot 5^e$ and $b = 3\cdot 5^f$, then $|\,a\,| = |\,b\,| = \omega$, but $a \neq b$; so by the linearity of the ordering by $<_o$ of the members of O which are $<_o$ a given one and the consistency of this ordering with that of the ordinals represented (end **20**), a and b cannot both occur among the numbers $<_o 2^{a\circ b}$. Another difficulty is that the associative law $(a+_o b)+_o c = a+_o(b+_o c)$ fails, e.g., when $a = 1$, $b = 2$, $c = 3\cdot 5^y$.

3. Assume $c = 3 \cdot 5^y$ where, for each n, $\Phi(y, n_O)$ is defined (call it y_n), $y_n \varepsilon O$ and $y_n <_O y_{n+1}$ (and by $O3$, $y_n <_O c$). Now it is Case 2 of (25.1) which applies to $\xi(a, w)$. Thus $\mathrm{Seq}(w)$, but w is not secured; moreover (as $y = f_{a,w}$), for each n, $y_n = \sum_{s<n}{}_O\, (\xi(a, w*2^{s+1}) +_O 1_O)$, so

$$\sum_{s<n}{}_O\, (\xi(a, w*2^{s+1}) +_O 1_O) \varepsilon O \text{ and } \sum_{s<n}{}_O\, (\xi(a, w*2^{s+1}) +_O 1_O) <_O c.$$

Using (XXII) and (XX), for every s, $\xi(a, w*2^{s+1}) \varepsilon O$. Furthermore, since (taking n above $= s+1$)

$$c >_O \sum_{m<s+1}{}_O\, (\xi(a, w*2^{m+1}) +_O 1_O)$$
$$= \sum_{m<s}{}_O\, (\xi(a, w*2^{m+1}) +_O 1_O) +_O (\xi(a, w*2^{s+1}) +_O 1_O),$$
$$|\, \xi(a, w*2^{s+1})| < |\, \xi(a, w*2^{s+1}) +_O 1_O\,| \leqq |\, \sum_{m<s+1}{}_O\, (\xi(a, w*2^{m+1}) +_O 1_O\,| < |\, c\,|.$$

So by the hypothesis of the transfinite induction, since $\xi(a, w*2^{s+1}) \varepsilon O$, $w*2^{s+1}$ is securable. This is for every s, and $\mathrm{Seq}(w)$, so w is securable.

COROLLARY. *The predicates $a \varepsilon O$ and $a <_O b$ are not expressible in the forms $(E\alpha)(x)R(a, \alpha, x)$ and $(E\alpha)(x)S(a, b, \alpha, x)$ with general recursive R and S, respectively; a fortiori, they are not arithmetical.*

Proof. Were $a \varepsilon O \equiv (E\alpha)(x)R(a, \alpha, x)$ with R recursive, by applying the theorem to $T_1{}^a(a, a, x)$ as its $R(a, \alpha, x)$, we would have

$$(\alpha)(Ex)T_1{}^a(a, a, x) \equiv (E\alpha)(x)R(\xi(a), \alpha, x) \equiv (E\alpha)(x)R_1(a, \alpha, x)$$

with recursive R_1, which is impossible.[30] The statement for $a <_O b$ follows, since $a \varepsilon O \equiv a <_O 2^a$ by $O2$ and (IV).

26. A digression concerning recursive linear orderings. Let us examine further the construction used in the proof of Theorem I.

We use $\succ$ to denote the linear ordering of the set $\hat{w}\,\mathrm{Seq}(w)$ of the numbers w of the form $\tilde{\alpha}(x)$ which is established by ordering the finite sequences $\alpha(0), \cdots, \alpha(x-1)$ lexicographically with the infinite alphabet $\cdots, 2, 1, 0$. In this ordering, 1 (which represents the empty sequence) is the highest element. If $\overline{\mathrm{Seq}}(u)$ or $\overline{\mathrm{Seq}}(v)$, $u \succ v$ shall be false. Then the predicate $u \succ v$ is primitive recursive.

Now, for any given predicate $R(a, v)$ and numbers a and w, we define a set $S^{R,a}{}_w$, or briefly $S^a{}_w$ or S_w, as follows. If w is secured (with respect to R and a), S_w shall be the unit set $\{w\}$. If $\mathrm{Seq}(w)$ and w is unsecured, S_w

[30] [12] Theorem 3 Proof for $n > 0$. Also cf. [12] Theorem 5.

shall consist of all $w*\tilde{\alpha}(t)$ which are unsecured or immediately secured. If $\overline{\text{Seq}}(w)$, S_w shall be the empty set. Then $u \varepsilon S^{R,a}_w$ as predicate of u, w, a is primitive recursive uniformly in R.

If $u \varepsilon S_w$, then Seq(u). So if Seq(w), S_w is linearly ordered by $\succ$ with w is highest element.

(F) *The set S_w is well-ordered by $\succ$, if w is securable, in which case the ordinal number of S_w is $|\xi(a,w)|+1$.*[31]

We prove this, as follows, by an induction of form corresponding to the inductive definition of securability.

1. Assume w is secured. Then S_w is $\{w\}$, which is well-ordered with ordinal number 1. But by Case 1 of (25.1), $\xi(a,w)=1=0_o$. So $|\xi(a,w)|+1=0+1=1$.

2. Assume Seq(w), w is unsecured, but $w*2^{s+1}$ is securable ($s=0,1,2,\cdots$), and as hypothesis of the induction that $S_{w*2^{s+1}}$ is well-ordered by $\succ$ with ordinal number $|\xi(a,w*2^{s+1})|+1$. Then under the ordering $\succ$, S_w is the sum of $\{w\},\cdots, S_{w*2^3}, S_{w*2^2}, S_{w*2^1}$, and so is well-ordered with the ordinal number $\sum_{s=0,1,2,\cdots}(|\xi(a,w*2^{s+1})|+1)+1$. But by Case 2 of (25.1),

$$\sum_{s=0,1,2,\cdots}(|\xi(a,w*2^{s+1})|+1)+1=|\xi(a,w)|+1.$$

(G) *If* Seq(w), *and S_w is well-ordered by $\succ$, then w is securable.*

For we can show by transfinite induction on the ordinal number of S_w that, if Seq(w), and S_w is well-ordered, then each member $w*\tilde{\alpha}(t)$ of S_w is securable; so in particular, then w $(=w*\tilde{\alpha}(0))$ is securable.

Now we return to (F), and give another argument for the part not concerning ξ, in which we show that, if S_w were not well-ordered by $\succ$, w would not be securable.

Accordingly suppose S_w is not well-ordered by $\succ$, so there there is an infinite descending sequence $\beta(0)\succ\beta(1)\succ\beta(2)\succ\cdots$ within S_w. Of course then Seq(w) and w is unsecured. Write $w=\bar{\gamma}(x)$ (then $x=\text{lh}(w)$).

Now we shall infer by induction on t that, for all sufficiently great m (say $m\geqq m_t$), $\text{lh}(\beta(m))>x+t$ and $(\beta(m))_x\dot{-}1,\cdots,(\beta(m))_{x+t}\dot{-}1$ are fixed in value (call their values then $\alpha(0),\cdots,\alpha(t)$, respectively). Let

[31] That S_w is well-ordered by $\succ$ if w is securable was argued in substance by Brouwer [1] Section 1 or [2] Section 2. For w securable, S_w consists of w and, if w is unsecured, those numbers $w*\tilde{\alpha}(t)$ coming below w in the lexicographic ordering $\succ$ which under the inductive definition of securability must be recognized as securable before w itself can be so recognized.

$n_t = m_{t-1}$ if $t > 0$ $(= 0$ if $t = 0)$, so that, using the hypothesis of the induction, for all $m \geqq n_t$, $\beta(m)$ represents a sequence the first $x + t$ values of which are fixed as $\gamma(0), \cdots, \gamma(x-1), \alpha(0), \cdots, \alpha(t-1)$. Then by the lexicographic ordering, for $m > n_t$, $\beta(m)$ must represent a sequence $\gamma(0), \cdots, \gamma(x-1), \alpha(0), \cdots, \alpha(t-1), (\beta(m))_{x+t} \dot{-} 1, \cdots, (\beta(m))_{\mathrm{lh}(\beta(m))-1} \dot{-} 1$ of length $> x + t$, and with increasing m $(m > n_t)$ $(\beta(m))_{x+t} \dot{-} 1$ is monotone non-increasing. But since $(\beta(m))_{x+t} \dot{-} 1$ is a natural number, starting with its value for $m = n_t + 1$, it can decrease only a finite number of times, so beginning with a certain value m_t $(> n_t)$ of m, $(\beta(m))_{x+t} \dot{-} 1$ remains fixed, call its value then $\alpha(t)$.

We can express α in terms of β and w by the formula [32]

$$\alpha(t) = (\varepsilon s(m)_{m \geqq (s)_0}[(\beta(m))_{\mathrm{lh}(w)+t} \dot{-} 1 = (s)_1])_1.$$

So α is arithmetical uniformly in β.[33]

Since $\beta(m_t)$ is of the form $w * \bar{\alpha}(t+1) * v$, and $\beta(m_t) \varepsilon S_w$, $w * \bar{\alpha}(t)$ and w are unsecured; a fortiori, $\bar{R}(a, w * \bar{\alpha}(t))$.

Thus $(E\alpha)(t)\bar{R}(a, w * \bar{\alpha}(t))$, whence $\overline{(\alpha)}(Et)R(a, w * \bar{\alpha}(t))$, besides which w is unsecured; so w is unsecurable.

So we have another proof of (F). In the course of this we have shown:

(H) *For each w, there is a function α arithmetical uniformly in β such that, if $\beta(0), \beta(1), \beta(2), \cdots \varepsilon S_w$ and $\beta(0) \succ \beta(1) \succ \beta(2) \succ \cdots$, then w is unsecured and $(t)\bar{R}(a, w * \bar{\alpha}(t))$.*

These results, of course, hold with $a_1, \cdots, a_n$ (for any fixed $n \geqq 0$) in place of a. Now we give an application with $w = 1$ and $n = 0$.

Elsewhere we have shown that there is a primitive recursive predicate $R(v)$ such that (a) $(E\alpha)(x)\bar{R}(\bar{\alpha}(x))$, but (b) for no arithmetical α, $(x)\bar{R}(\bar{\alpha}(x))$.[34] Consider the set $S^R{}_1$ or briefly S_1. By (a), $\overline{(\alpha)}(Ex)R(\bar{\alpha}(x))$, i.e., 1 is not securable, so by (G), S_1 is not well-ordered by $\succ$, so there is a β such that $\beta(0), \beta(1), \beta(2), \cdots \varepsilon S_1$ and $\beta(0) \succ \beta(1) \succ \beta(2) \succ \cdots$. But were there such a β which was arithmetical, the corresponding α of (H) would be an arithmetical function such that $(x)\bar{R}(\bar{\alpha}(x))$, contradicting (b).

The set S_1 is primitive recursive and infinite, and $0 \notin S_1$ but $1 \varepsilon S_1$.

---

[32] As in [7] or [11] p. 317 (following Gödel) $\varepsilon s A(s) = \{$the least s such that $A(s)\}$ if $(Es)A(s)$, $= 0$ otherwise.

[33] [11] pp. 239, 291, 292, or [12] Section 2. A function α is arithmetical (arithmetical in β), if its representing predicate $\alpha(x) = w$ is arithmetical (arithmetical in β). Cf. [11] pp. 285, 318.

[34] [12] Corollary to Theorem 7. We are rewriting the $(x)R(\alpha, x)$ there as $(x)\bar{R}(\bar{\alpha}(x))$ (cf. beginning 24 above and [11] p. 228 #D).

Let $\sigma(0) = 1$, $\sigma(n+1) = n+1$ if $n+1 \varepsilon S_1$, and $\sigma(n+1) = \sigma(n)$ if $n+1 \notin S_1$. Then σ is primitive recursive, and $\sigma(0), \sigma(1), \sigma(2), \cdots$ is an enumeration of S_1 with only consecutive repetitions. Now define

$$i >^R j \equiv [\sigma(i) \neq \sigma(j) \,\&\, \sigma(i) \succ \sigma(j)] \vee [\sigma(i) = \sigma(j) \,\&\, i > j].$$

Then $i >^R j$ is a primitive recursive linear ordering of the natural numbers, and members of S_1 are ordered by $>^R$ as they are by $\succ$.

So for any infinite descending sequence $\beta(0) \succ \beta(1) \succ \beta(2) \succ \cdots$ within S_1, $\beta(0) >^R \beta(1) >^R \beta(2) >^R \cdots$. Thus there is an infinite descending sequence in the ordering $>^R$ of the natural numbers.

But there is none which is arithmetical. For given any γ such that $\gamma(0) >^R \gamma(1) >^R \gamma(2) >^R \cdots$, let $\psi(0) = 0$ and

$$\psi(n+1) = \mu t_{t > \psi(n)} [\sigma(\gamma(t)) \neq \sigma(\gamma(\psi(n)))],$$

and let $\beta(n) = \sigma(\gamma(\psi(n)))$. Then β is general recursive, a fortiori arithmetical, in γ, and $\beta(0) \succ \beta(1) \succ \beta(2) \succ \cdots$ is an infinite descending sequence within S_1. Thus we have established:

(J) *There is a primitive recursive linear ordering $>^R$ of the natural numbers such that, for some number-theoretic function γ,*

$$\gamma(0) >^R \gamma(1) >^R \gamma(2) >^R \cdots,$$

but, for every arithmetical γ, $(En)[\gamma(n) \leqq^R \gamma(n+1)]$.

In other words, $>^R$ is a well-ordering of the natural numbers with respect to arithmetical sequences $\gamma(0), \gamma(1), \gamma(2), \cdots$, but not with respect to arbitrary sequences.[35]

In fact, the primitive recursive $R(v)$ can be chosen so that $>^R$ is a well-ordering with respect to a much larger class C of sequences $\gamma(0), \gamma(1), \gamma(2), \cdots$ than the arithmetical sequences, but not with respect to arbitrary sequences.[36]

---

[35] G. Kreisel raised (in a different formulation) the question whether this is the case in a letter to the author dated December 9, 1952 (in reply to a letter from the author dated November 13, 1952, in which the result of [12] which leads here to (J) was stated), and also in a communication received by Leon Henkin November 20, 1952. Kreisel formulated the question in relation to the formal system Z_μ of Hilbert-Bernays [5] and some ω-consistent formal system S of analysis including Z_μ, while here we have considered the matter only informally. The arithmetical functions are however exactly those expressible by terms of Z_μ under the usual interpretation of the symbolism, and our arguments about arbitrary number-theoretic functions can presumably be formalized in a formal system S of analysis of a usual sort.

[36] We need only start from Theorems 7 and 9 of [12] (instead of from Corollary

27. Reduction of $a \varepsilon Q$ (amended). Now we begin the proof that $a \varepsilon O \equiv (\alpha)(Ey)R(a, \alpha, y)$ for a suitable primitive recursive R. As before, we start from

$$a \varepsilon O \equiv a \varepsilon Q \tag{28}$$

(end **12**) and (32) (in **13**, **20**). But now we amend the former treatment (cf. **14**) so that we shall be able to give (in **28**) the necessary argument to supplement the application of the reduction technique (cf. **18**).

The inductive definition of Q (in **12**) can be restated as follows (cf. beginning **14**[11]).

$Q_1 1$. If $a = 1$, then $a \varepsilon Q$. $Q_1 2$. If $a = 2^{(a)_0} \,\&\, (a)_0 \varepsilon Q$, then $a \varepsilon Q$. $Q_1 3$. If

$$\begin{aligned} a = 3 \cdot 5^{(a)_2} \,\&\, & (x_0)(Ey_0)T((a)_2, (x_0)_0, y_0) \\ & \&\, (x_0)(x_1)[T((a)_2, (x_0)_0, x_1) \to U(x_1) \varepsilon Q] \\ & \&\, (x_0)(x_1)(x_2)[T((a)_2, (x_0)_0, x_1) \\ & \&\, T((a)_2, (x_0 + 1)_0, x_2) \to (Ey_1)V(U(x_1), U(x_2), y_1)], \end{aligned}$$

then $a \varepsilon Q$. $Q_1 4$. $a \varepsilon Q$ only as required by $Q_1 1$-$Q_1 3$.

By writing a corresponding equivalence (as we did for various inductive definitions in the first paper; cf. **18** here), and then substituting in it for "$a \varepsilon Q$" the predicate expression "$(\alpha)(Ey)R(a, \bar{\alpha}(y))$" where $R(a, v)$ remains to be selected, we obtain

$$\begin{aligned} (\alpha)(Ey)R(a, \bar{\alpha}(y)) \equiv\ & a = 1 \vee \{a = 2^{(a)_0} \,\&\, (\alpha)(Ey)R((a)_0, \bar{\alpha}(y))\} \\ & \vee \{a = 3 \cdot 5^{(a)_2} \,\&\, (x_0)(Ey_0)T((a)_2, (x_0)_0, y_0) \,\&\, (x_0)(x_1)[T((a)_2, (x_0)_0, x_1) \\ & \to (\alpha)(Ey)R(U(x_1), \bar{\alpha}(y))] \,\&\, (x_0)(x_1)(x_2)[T((a)_2, (x_0)_0, x_1) \\ & \&\, T((a)_2, (x_0 + 1)_0, x_2) \to (Ey_1)V(U(x_1), U(x_2), y_1)]\}. \end{aligned} \tag{27.1}$$

We shall presently define $R(a, v)$ so that it will be primitive recursive and (27.1) will be true. When this has been done, it will follow from (27.1) by an induction of form corresponding to the inductive definition $Q_1 1$-$Q_1 4$ (cf. **18**) that

$$a \varepsilon Q \to (\alpha)(Ey)R(a, \bar{\alpha}(y)). \tag{27.2}$$

---

to Theorem 7) to obtain as C, for any fixed $y \varepsilon O$, the sequences recursive in the predicate H_y of [12] Section 6; we apply Theorem 7 to $H_{y+_o 2_o}$ to allow for the definition of α from β for (H). In [13] XXVI we obtain (with the aid of Theorem II below) an improvement over [12] Theorem 7, using which C can be the sequences recursive in H_y for any $y \varepsilon O$.

Note that, if C and D are independent of α,

$$(27.3) \qquad \begin{aligned} \bar{C} \vee \bar{D} \rightarrow \{&(\alpha)(C \& A(\alpha)) \vee (\alpha)(D \& B(\alpha)) \\ &\equiv (\alpha)[(C \& A(\alpha)) \vee (D \& B(\alpha))]\}. \end{aligned}$$

To find a primitive recursive $R(a, v)$ satisfying (27.1), we begin by observing that in the right member of (27.1) (call it (a)) the quantifiers can be advanced (using (27.3) to bring both (α)'s across the second $\vee$ as one (α)))[37] to give an equivalent of the form

(b) $$(x_0)(x_1)(x_2)(\alpha)(Ey_0)(Ey_1)(Ey)M^R(a, x_0, x_1, x_2, \bar{\alpha}(y), y_0, y_1)$$

where $M^R(a, x_0, x_1, x_2, \bar{\alpha}(y), y_0, y_1)$ is exactly (a) with its quantifiers omitted. Next (b) is equivalent to[38]

(c) $$\begin{aligned} (\alpha)(Ey)\{&M^R(a, \alpha(0), \alpha(1), \alpha(2), \\ &\{\overline{\lambda i \alpha(i+3)}\}((y \dot{-} 3)_2), (y \dot{-} 3)_0, (y \dot{-} 3)_1) \& y \geqq 3\}. \end{aligned}$$

But $y = \mathrm{lh}(\bar{\alpha}(y))$, and for $y \geqq 3$,

$$\alpha(0) = (\bar{\alpha}(y))_0 \dot{-} 1, \alpha(1) = (\bar{\alpha}(y))_1 \dot{-} 1, \alpha(2) = (\bar{\alpha}(y))_2 \dot{-} 1$$

and (since $y \geqq 3 \& i < (y \dot{-} 3)_2 \rightarrow i + 3 < y$)

$$\{\overline{\lambda i \alpha(i+3)}\}((y \dot{-} 3)_2) = \prod_{i < (y \dot{-} 3)_2} p_i \exp(\bar{\alpha}(y))_{i+3},$$

using which (c) takes the form $(\alpha)(Ey)N^R(a, \bar{\alpha}(y))$ (call it (d)). Now we propose to define R by

$$(27.4) \qquad R(a, v) \equiv N^R(a, v).$$

This does define a predicate $R(a, v)$ by course-of-values recursion on v, since for $\mathrm{lh}(v) < 3$ it makes $R(a, v)$ false outright, while for $\mathrm{lh}(v) \geqq 3$ it makes $R(a, v)$ depend primitive recursively on $R(b, w)$ only for

$$w = \prod_{i < (\mathrm{lh}(v) \dot{-} 3)_2} p_i \exp(v)_{i+3} < v.$$

The predicate $R(a, v)$ thus defined is primitive recursive.[39] Substituting into (27.4) and quantifying,

$$(27.5) \qquad (\alpha)(Ey)R(a, \bar{\alpha}(y)) \equiv (\alpha)(Ey)N^R(a, \bar{\alpha}(y)),$$

---

[37] See **14** p. 54 for justification of the advances intuitionistically.

[38] By [12] Footnote 7, and a modification of **5** (16),[11] [9] (15) or [11] p. 285 (17). Following Church, $\lambda i f(i)$ is $f(i)$ as a function of i (cf. [11] p. 34).

[39] One can eliminate both the course-of-values character of the recursion on v and the substitution for the parameter a by the methods of Péter [17] Sections 1 and 2 or [18] Sections 3 and 5. Actually by beginning **24** it would suffice for our results to observe merely that $R(a, v)$ is general recursive, which is obvious.

whence by reversing the steps from (a) to (d) we now prove (27.1) and thence (27.2) for the R defined by (27.4).

28. Supplementary argument to the reduction of $a \varepsilon Q$. We prove that

$$(28.1) \qquad (\alpha)(Ey)R(a, \bar{\alpha}(y)) \rightarrow a \varepsilon Q,$$

conversely to (27.2). So assume for a given a that $(\alpha)(Ey)R(a, \bar{\alpha}(y))$ for the R defined by (27.4). Then by **24**, 1 is securable with respect to (R and) a; and by **26** (F), the set $S^{R,a}{}_1$ or briefly $S^a{}_1$ is well-ordered by $\succ$, say with the ordinal number $|S^a{}_1|$ $(= |\xi(a,1)| + 1)$. We use transfinite induction on this number.[40] By our assumption and (27.1), one of three cases applies.

1. $a = 1$. Then $a \varepsilon Q$, by $Q_1 1$.

2. $a = 2^{(a)_0} \,\&\, (\alpha)(Ey)R((a)_0, \bar{\alpha}(y))$. By **24**, 1 is securable with respect to $(a)_0$. For any x_0, x_1, x_2, α, let y^α be the least y such that $R((a)_0, \bar{\alpha}(y))$, so $\bar{\alpha}(y^\alpha)$ is immediately secured with respect to $(a)_0$; and consider some function β with $\beta(3 + y^\alpha) = [x_0, x_1, x_2] * \bar{\alpha}(y^\alpha)$, where $[x_0, \cdots, x_n]$ abbreviates $p_0{}^{x_0+1} \cdots p_n{}^{x_n+1}$. For $z < 3$, $\bar{R}(a, \beta(z))$ immediately by the definition of $R(a,v)$, and for $3 \leqq z < 3 + y^\alpha$ because $R(a, \bar{\beta}(z))$ would imply $R((a)_0, \bar{\alpha}((z \dot{-} 3)_2))$ with $(z \dot{-} 3)_2 < y^\alpha$ contradicting the choice of y^α; but we can choose $z \geqq 3 + y^\alpha$ so that $(z \dot{-} 3)_2 = y^\alpha$, and then $R(a, \bar{\beta}(z))$. Thus there is a u such that $[x_0, x_1, x_2] * \bar{\alpha}(y^\alpha) * u$ is immediately secured with respect to a (namely $\bar{\beta}(\mu z R(a, \bar{\beta}(z))) / \bar{\beta}(3 + y^\alpha)$). So $S^a{}_{[x_0,x_1,x_2]}$ includes all the numbers $[x_0, x_1, x_2] * w$ for $w \varepsilon S^{(a)_0}{}_1$, hence $|S^a{}_{[x_0,x_1,x_2]}| \geqq |S^{(a)_0}{}_1|$. Moreover, under the ordering $\succ$, $S^a{}_{[x_0,x_1]}$ is the sum of $\{[x_0, x_1]\}$ and the sets $S^a{}_{[x_0,x_1,x_2]}$ for $x_2 = \cdots, 2, 1, 0$, hence $|S^a{}_{[x_0,x_1]}| \geqq \omega |S^{(a)_0}{}_1| + 1$; etc. So finally $|S^a{}_1| \geqq \omega(\omega(\omega |S^{(a)_0}{}_1| + 1) + 1) + 1 > |S^{(a)_0}{}_1|$. So by the hypothesis of the induction, $(a)_0 \varepsilon Q$. By $Q_1 2$, $a \varepsilon Q$.

3. $a = 3 \cdot 5^{(a)_2} \,\&\, (x_0)(Ey_0)T((a)_2, (x_0)_0, y_0) \,\&\, (x_0)(x_1)[T((a)_2, (x_0)_0, x_1)$
$\rightarrow (\alpha)(Ey)R(U(x_1), \bar{\alpha}(y))] \,\&\, (x_0)(x_1)(x_2)[T((a)_2, (x_0)_0, x_1)$
$\& T((a)_2, (x_0 + 1)_0, x_2) \rightarrow (Ey_1)V(U(x_1), U(x_2), y_1)]$.

In particular, for each x_0 and x_1 such that $T((a)_2, (x_0)_0, x_1)$, 1 is securable with respect to $U(x_1)$. For any such x_0, x_1 fixed for the moment, and any x_2, α, let y^α be the least y such that $R(U(x_1), \bar{\alpha}(y))$, so $\bar{\alpha}(y^\alpha)$ is immediately

[40] There is a longer proof, which avoids the use of the classical second number class, and uses instead (E) and an induction corresponding to the inductive definition of securability.

secured with respect to $U(x_1)$; and consider some function β with $\bar{\beta}(3+y^\alpha) = [x_0, x_1, x_2]*\bar{\alpha}(y^\alpha)$. For $z<3$, $\bar{R}(a,\beta(z))$ obviously, and for $3 \leqq z < 3+y^\alpha$ because $R(a,\bar{\beta}(z))$ would imply $R(U(x_1), \bar{\alpha}((z \dot{-} 3)_2))$ with $(z \dot{-} 3)_2 < y^\alpha$ contradicting the choice of y^α; but we can choose $z \geqq 3+y^\alpha$ so that $(z \dot{-} 3)_2 = y^\alpha$, $T((a)_2, (x_0)_0, (z \dot{-} 3)_0)$ and

$$T((a)_2, (x_0+1)_0, x_2) \to V(U(x_1), U(x_2), (z \dot{-} 3)_1),$$

and then $R(a,\bar{\beta}(z))$. Thus there is a u such that $[x_0, x_1, x_2]*\bar{\alpha}(y^\alpha)*u$ is immediately secured with respect to a. Hence $|S^a{}_1| \geqq \omega\,|S^{U(x_1)}{}_1| + 3 > |S^{U(x_1)}{}_1|$. So applying the hypothesis of the induction,

$$(x_0)(x_1)[T((a)_2, (x_0)_0, x_1) \to U(x_1) \varepsilon Q].$$

By $Q_1 3$, $a \varepsilon Q$.[41]

29. Classification of $a \varepsilon O$ and $a <_o b$ from above.

THEOREM II. *For certain primitive recursive predicates R and S, $a \varepsilon O \equiv (\alpha)(Ey)R(a,\alpha,y)$ and $a <_o b \equiv (\alpha)(Ey)S(a,b,\alpha,y)$.*

Proof. Letting $R(a,\alpha,y) \equiv R(a,\bar{\alpha}(y))$ for the $R(a,v)$ defined by (27.4), and combining (28) (**12** or **27**) with (27.2) and (28.1),

$$a \varepsilon O \equiv (\alpha)(Ey)R(a,\alpha,y). \tag{29.1}$$

By (IV) (**12** or **20**) with (21.1),

$$a <_o b \equiv b \varepsilon O\ \&\ (Ex)V(a,b,x), \tag{29.2}$$

which with (29.1) by advancing and contracting quantifiers gives

$$a <_o b \equiv (\alpha)(Ey)[R(b,\alpha,(y)_0)\ \&\ V(a,b,(y)_1)]. \tag{29.3}$$

30. The predicates $a \varepsilon O^P$ and $a <_o{}^P b$. The definitions of the predicates $a \varepsilon O$ and $a <_o b$ and the representation of ordinals can be relativized by using recursiveness in a given predicate $P(a)$ in place of recursiveness.[42] To do this, we simply read throughout the first three and last paragraphs of **20** "T^P", "$T_1{}^P$", "Φ^P", "$\Phi_1{}^P$", "recursively from P", "O^P", "$<_o{}^P$", "$|\ |^P$", "$\omega_1{}^P$" for "T", "T_1", "Φ", "Φ_1", "recursively", "O", "$<_o$", "$|\ |$", "ω_1", respectively.[43] The resulting notions O^P, $<_o{}^P$, $|\ |^P$, $\omega_1{}^P$ (e.g.,

[41] By this proof and **27**, $a \varepsilon O \to |S^a{}_1| \geqq |a|$.

[42] Or indeed in any given list Ψ of l functions and predicates of $m_1, \cdots, m_l$ variables, respectively.

[43] For $T_1{}^P$, $\Phi_1{}^P$, or what is the same $T_1{}^\pi$, $\Phi_1{}^\pi$ where π is the representing function of P, cf. [11] pp. 227, 292, 341.

for $P(a) \equiv a \varepsilon O$) are discussed in [12] 6.4 ff. and [13] Section 7 (also cf. [14] end 3.5).

The above arguments carry over to these relativized notions. For the most part, the changes required in the text are only the supplying of superscripts "^{P}" on the symbols for various functions, predicates and sets, and the reading of "recursive in P" (which can often be "recursive uniformly in P") in place of "recursive".

Thus in **20** and **21**, then T^P, V^P, enm^P and $m <_b{}'^P n$ are primitive, and Φ^P and $m <_b{}^P n$ partial, recursive uniformly in P (but n_0, $\mathrm{Fin}(b)$ and $\mathrm{nat}(b)$ do not change). In **22** and **23** we have a function $+_o{}^1$ and operation $\sum o^{1}$,[44] which are still primitive recursive (in Case 3 for (22.1), $d_{a,y}$ defines recursively $a +_o{}^1 \Phi^P(y, n_0)$ as a function of n_0 uniformly from P; $\theta^P(z, a, y, n) \cong \Phi_2(z, a, \Phi^P(y, n))$; p^1 is a uniform Gödel number from P of $\theta^P(z, a, y, n)$; in (22.2) $S_1{}^3$ becomes $S_1{}^{3,1}$). In **24**, using $(Ex)R^P(a, \alpha, x) \equiv (Ex)T_1{}^{1,1}(\bar{\pi}(x), \bar{\alpha}(x), f, a)$ for π the representing function of P, any predicate of the form $(Ex)R^P(a, \alpha, x)$ with R^P general recursive in P is expressible as $(Ex)R^P(a, \bar{\alpha}(x))$ with an R^P primitive recursive in P (uniformly so, if $R^P(a, \alpha, x)$ was); and the definitions of 'secured' etc. are considered with respect to R^P and a (but $\mathrm{Seq}(w)$ does not change). In **25** Theorem I becomes: *Given any predicate $R^P(a, \alpha, x)$ general recursive in P (uniformly in P), a function $\xi^P(a)$ primitive recursive in P (uniformly in P) can be found such that* $(\alpha)(Ex)R^P(a, \alpha, x) \equiv \xi^P(a) \varepsilon O^P$. In **26** $\succ$ is unchanged; and replacing R by R^P in our arguments, (J) gives a linear ordering $>^{R^P}$, primitive recursive in P, which is a well-ordering with respect to sequences $\gamma(0), \gamma(1), \gamma(2), \cdots$ arithmetical in P, but not with respect to arbitrary sequences. In **27-29**, starting from $a \varepsilon O^P \equiv a \varepsilon Q^P$, we obtain as the relative version of Theorem II: *For certain predicates R^P and S^P primitive recursive uniformly in P,*

$$a \varepsilon O^P \equiv (\alpha)(Ey)R^P(a, \alpha, y) \quad \textit{and} \quad a <_o{}^P b \equiv (\alpha)(Ey)S^P(a, b, \alpha, y).$$

THE UNIVERSITY OF WISCONSIN.

---

[44] The superscript "1" is for the number 1 of the arguments of P; were we relativizing to Ψ we would have $+_o{}^{m_1, \ldots, m_l}$, $\sum o^{m_1, \ldots, m_l}$.[42]

BIBLIOGRAPHY.

[1] L. E. J. Brouwer, "Beweis, dass jede volle Funktion gleichmässig stetig ist," *Koninklijke Nederlandsche Akademie van Wetenschappen, Proceedings of the Section of Sciences*, vol. 27 (1924), pp. 189-193.

[2] ———, "Über Definitionsbereiche von Funktionen," *Mathematische Annalen*, vol. 97 (1927), pp. 60-75.

[3] A. Church, "The constructive second number class," *Bulletin of the American Mathematical Society*, vol. 44 (1938), pp. 224-232.

[4] A. Church and S. C. Kleene, "Formal definitions in the theory of ordinal numbers," *Fundamenta Mathematicae*, vol. 28 (1936), pp. 11-21.

[5] D. Hilbert and P. Bernays, *Grundlagen der Mathematik*, Berlin, vol. 2 (1939).

[6] L. Kalmár, "Egyszerü példa eldönthetetlen aritmetikai problémára (Ein einfaches Beispiel für ein unentscheidbares arithmetisches Problem)," *Matematikai és Fizikai Lapok*, vol. 50 (1943), pp. 1-23.

[7] S. C. Kleene, "General recursive functions of natural numbers," *Mathematische Annalen*, vol 112 (1936), pp. 727-742.

[8] ———, "On notation for ordinal numbers," *Journal of Symbolic Logic*, vol. 3 (1938), pp. 150-155.

[9] ———, "Recursive predicates and quantifiers," *Transactions of the American Mathematical Society*, vol. 53 (1943), pp. 41-73 (cf. **19** above).

[10] ———, "Recursive functions and intuitionistic mathematics," *Proceedings of the International Congress of Mathematicians (Cambridge, Mass., U. S. A., Aug. 30-Sept. 6, 1950)*, 1952, vol. 1, pp. 679-685.

[11] ———, *Introduction to Metamathematics*, New York, Toronto, Amsterdam and Groningen (1952).[23]

[12] ———, "Arithmetical predicates and function quantifiers," forthcoming in *Transactions of the American Mathematical Society*.

[13] ———, "Hierarchies of number-theoretic predicates," forthcoming in *Bulletin of the American Mathematical Society*.

[14] S. C. Kleene and Emil L. Post, "The upper semi-lattice of degrees of recursive unsolvability," *Annals of Mathematics*, ser. 2, vol. 59 (1954), pp. 379-407.

[15] W. Markwald, "Zur Theorie der konstruktiven Wohlordnungen," *Mathematische Annalen*, vol. 127 (1954), pp. 135-149.

[16] D. Nelson, "Recursive functions and intuitionistic number theory," *Transactions of the American Mathematical Society*, vol. 61 (1947), pp. 307-368.

[17] R. Péter, "Über den Zusammenhang der verschiedenen Begriffe der rekursiven Funktion," *Mathematische Annalen*, vol. 110 (1934), pp. 612-632.

[18] ———, *Rekursive Funktionen*, Budapest (1951).

[19] E. L. Post, "Recursively enumerable sets of positive integers and their decision problems," *Bulletin of the American Mathematical Society*, vol. 50 (1944), pp. 284-316.

[20] A. M. Turing, "Systems of logic based on ordinals," *Proceedings of the London Mathematical Society*, ser. 2, vol. 45 (1939), pp. 161-228.

LIE GROUPS AND LIE HYPERALGEBRAS OVER A FIELD OF CHARACTERISTIC $p > 0$ (IV).*

By JEAN DIEUDONNÉ.

---

1. Introduction. In this paper, we develop to their full generality the methods introduced in [4] and [5], which enable us to round off, in a way, the theory of abelian Lie groups over a field K. More precisely, we show that this theory is entirely equivalent to the study of finitely generated *modules* of a certain type over a certain ring $\mathfrak{A}$ and of their homomorphisms (Theorems 3 and 5). If, for simplicity's sake, we suppose K perfect, then $\mathfrak{A}$ is defined in the following way: let $\mathfrak{R}$ be the ring of integers in the complete unramified p-adic field $\mathfrak{K}$ having K as its field of residues; then $\mathfrak{A}$ is the ring of *non commutative power series* $\boldsymbol{r}_0 + T\boldsymbol{r}_1 + \cdots + T^n\boldsymbol{r}_n + \cdots$, where $\boldsymbol{r}_n \in \mathfrak{R}$ and $\boldsymbol{r}T = T\boldsymbol{r}^\sigma$ for every $\boldsymbol{r} \in \mathfrak{R}$, σ being the automorphism of $\mathfrak{R}$ which corresponds to the automorphism $\xi \to \xi^p$ of K in the usual way. The ring $\mathfrak{A}$ is not a principal (noncommutative) ideal ring, and this accounts for the fact that the theory cannot yet be considered as complete, there being, as far as I know, no satisfactory theory of finitely generated modules over such a ring; but at least the kind of difficulties which lie in the way is now clearly delimited.

The main technical tools, as in [5], are the *hyperexponential group* and direct products of finite numbers of such groups; their role as "universal groups" stems from the fundamental fact that their hyperalgebra is *free* (in other words, it is an algebra of polynomials). For technical reasons, it is sometimes easier to work with the (additive) *Witt group*, which is isomorphic to the hyperexponential group, but is more convenient for some computations. It may be hoped that these tools will also one day be useful in the, apparently much more difficult, study of noncommutative formal Lie groups over a field of characteristic p.

2. The ring of endomorphisms of the Witt group. Owing to the close relationship between the (additive) Witt group and p-adic rings, it will be technically more convenient to determine first the endomorphisms of the Witt group; the determination of the endomorphisms of any group of hyperexponential type will then be quite trivial, since such a group is isomorphic to the Witt group [5, no. 7].

---

* Received January 20, 1955.

We do not repeat here the definition of the additive Witt group W (see for instance [5, no. 7], or [6, no. 2]); it is a recursive group over the weighted variables x_i ($i \geq 0$), x_i having the weight p^i. We shall write $\boldsymbol{\phi} = (\phi_0, \phi_1, \cdots, \phi_i, \cdots)$ its group law, $\phi_i(\boldsymbol{x}, \boldsymbol{y})$ being an isobaric polynomial of total weight p^i in $x_0, \cdots, x_i, y_0, \cdots, y_i$; more precisely, one has

$$\phi_i(\boldsymbol{x}, \boldsymbol{y}) = x_i + y_i + \psi_i(x_0, y_0, x_1, y_1, \cdots, x_{i-1}, y_{i-1}),$$

and the coefficients of ψ_i are in the prime field $\boldsymbol{F}_p$.

We can of course consider W as a group over *any* field K of characteristic p; but the notion of endomorphism of W depends on K, and we will say that $\boldsymbol{u} = (u_0, u_1, \cdots, u_i, \cdots)$ is a *K-endomorphism* of W if the coefficients of the formal power series u_i are in K. We will write $\mathcal{E}(K)$, or simply $\mathcal{E}$, for the set of K-endomorphisms of W which are *recursive*, that is, such that $u_i(\boldsymbol{x})$ only contains the indeterminates $x_0, x_1, \cdots, x_i$; on the other hand, we depart here from the conventions made in [5, no. 2] in that *we do not assume* that the minimum weight of u_i tends to $+\infty$ with i; this can be done here, due to the fact that ϕ_i and u_i contain a finite number of indeterminates. The set $\mathcal{E}(K)$ can then be made into a *ring* in the usual fashion, $\boldsymbol{uv}$ meaning the composite endomorphism $\boldsymbol{x} \to \boldsymbol{u}(\boldsymbol{v}(\boldsymbol{x}))$, and $\boldsymbol{u} + \boldsymbol{v}$ the endomorphism $\boldsymbol{w}$ such that $\boldsymbol{w}(\boldsymbol{x})$ is obtained by taking the "product" in W of $\boldsymbol{u}(\boldsymbol{x})$ and $\boldsymbol{v}(\boldsymbol{x})$; in other words, we have

$$w_i(\boldsymbol{x}) = \phi_i(u_0(\boldsymbol{x}), \cdots, u_i(\boldsymbol{x}); v_0(\boldsymbol{x}), \cdots, v_i(\boldsymbol{x})) \qquad (i = 0, 1, \cdots).$$

3. In order to study the structure of the ring $\mathcal{E}(K)$, we first consider certain special types of endomorphisms of W:

1. The "Frobenius homomorphism" $\boldsymbol{p}$, such that

$$p_i(\boldsymbol{x}) = x_i^p \qquad (i = 0, 1, \cdots). \tag{1}$$

2. The "shift" homomorphism $\boldsymbol{t}$, such that

$$t_0(\boldsymbol{x}) = 0, \qquad t_i(\boldsymbol{x}) = x_{i-1} \qquad (i = 1, 2, \cdots). \tag{2}$$

It is well-known [7] that the product

$$\boldsymbol{\pi} = \boldsymbol{tp} = \boldsymbol{pt} \tag{3}$$

is the "p-th-power endomorphism" of the group W, and we have

$$\pi_0(\boldsymbol{x}) = 0, \qquad \pi_i(\boldsymbol{x}) = x_{i-1}^p \qquad (i = 1, 2, \cdots). \tag{4}$$

3. Let $\mathfrak{W}(K)$ be the ring of *Witt-vectors* $A = (a_0, a_1, \cdots, a_i, \cdots)$ *over*

K; it is a commutative ring of characteristic 0 without zero divisors, with unit $I = (1, 0, \cdots, 0, \cdots)$ [7]. To each such vector A corresponds an endomorphism

$$\boldsymbol{x} \to A \cdot \boldsymbol{x} \tag{5}$$

of the additive group W, the "product" being taken in the sense of the Witt *multiplicative* group; $y_i = (A \cdot \boldsymbol{x})_i$ is an isobaric polynomial in $x_0, \cdots, x_i$, of weight p^i, with coefficients in K. If in y_i we substitute 1 for x_0, 0 for all x_j of index $j \geq 1$, we obtain the i-th component a_i of A; therefore there is a one-to-one correspondence between the Witt-vectors A and the endomorphisms (5) they define in W, and this correspondence is in fact a ring-isomorphism between $\mathfrak{W}(K)$ and the corresponding subring of $\mathfrak{E}(K)$. We shall from now on *identify* these two rings. The endomorphism $\boldsymbol{\pi}$ is then identified with the element $p \cdot I = (0, 1, 0, \cdots, 0, \cdots)$ of $\mathfrak{W}(K)$; $\mathfrak{W}(K)$ is a complete valuation ring, the valuation $\omega(A)$ being the smallest index i such that $a_i \neq 0$; the field of residues is K, and when K is perfect, $\mathfrak{W}(K)$ is isomorphic to the unique unramified complete valuation ring having K as its field of residues [7]. We define a ring-endomorphism σ of $\mathfrak{W}(K)$ by putting

$$A^\sigma = (a_0^p, a_1^p, \cdots, a_i^p, \cdots) \tag{6}$$

With this definition, it is readily verified that we have the commutation laws

$$\boldsymbol{p}A = A^\sigma \boldsymbol{p}, \qquad A\boldsymbol{t} = \boldsymbol{t}A^\sigma. \tag{7}$$

We also notice that the series

$$A_0 + A_1\boldsymbol{p} + \cdots + A_k\boldsymbol{p}^k + \cdots \tag{8}$$

$$B_0 + \boldsymbol{t}B_1 + \boldsymbol{t}^2B_2 + \cdots + \boldsymbol{t}^kB_k + \cdots \tag{9}$$

represent meaningful endomorphisms, when the A_k and B_k are arbitrary elements of the ring $\mathfrak{W}(K)$; indeed, the j-th component of $(A_k\boldsymbol{p}^k) \cdot \boldsymbol{x}$ is an isobaric polynomial in $x_0, \cdots, x_j$, of weight p^{j+k}; it follows that, if $\boldsymbol{s}_k$ is the sum of the first k terms of (8), the terms of weight $< p^k$ in any component of $\boldsymbol{s}_k(\boldsymbol{x})$ are the same as in the component of $\boldsymbol{s}_{k+1}(\boldsymbol{x})$ of the same index. On the other hand, any component of $(\boldsymbol{t}^kB_k) \cdot \boldsymbol{x}$ of index $\leq k$ is 0; therefore, if $\boldsymbol{u}_k$ is the sum of the first k terms of (9), the components of $\boldsymbol{u}_k(\boldsymbol{x})$ of index $\leq k$ are the same as those of $\boldsymbol{u}_{k+1}(\boldsymbol{x})$, and this proves our assertion.

It follows from (7) that the series (8) (resp. (9)) is invertible in $\mathfrak{E}(K)$ if and only if A_0 (resp. B_0) is invertible in $\mathfrak{W}(K)$, which means that $\omega(A_0) = 0$, or equivalently that if $A_0 = (a_{00}, a_{01}, \cdots, a_{0i}, \cdots)$, we have $a_{00} \neq 0$ in K. The inverse is computed in the usual way, as another power

series of type (8), whose coefficients are determined recursively by those of (8). The results are similar for (9).

4. We can now characterize the elements of $\mathfrak{E}(K)$:

THEOREM 1. *If K is perfect, every endomorphism $u \in \mathfrak{E}(K)$ can be written in one and only one way in the form*

$$u = \sum_{k=0}^{\infty} A_k p^k + \sum_{k=1}^{\infty} t^k B_k \tag{10}$$

where the A_k and B_k are elements of the ring $\mathfrak{W}(K)$.

Writing that u is an endomorphism, we obtain first the relation

$$u_0(x_0 + y_0) = u_0(x_0) + u_0(y_0)$$

from which the form of u_0 follows trivially:

$$u_0(x_0) = a_0 x_0 + a_1 x_0^p + \cdots + a_k x_0^{p^k} + \cdots.$$

Let $A_i = (a_i, 0, 0, \cdots)$ for each i, and consider the endomorphism $v_0 = A_0 + A_1 p + \cdots + A_k p^k + \cdots$; it is clear that $u_0(x_0) = v_{00}(x_0)$, and therefore the endomorphism $w = u - v_0$ is such that $w_0(x_0) = 0$.

As a basis for an inductive argument, let us now suppose that we have $u_j(x) = 0$ for $j < i$, and let us determine $u_i(x)$. We must have

$$u_i(x_0, \cdots, x_i) + u_i(y_0, \cdots, y_i) = u_i(x_0 + y_0, \phi_1(x, y), \cdots, \phi_i(x, y)). \tag{11}$$

On the other hand, we have $\pi u = u\pi$, and this, using the inductive hypothesis and relations (4), gives

$$u_i(0, x_0^p, \cdots, x_{i-1}^p) = 0, \tag{12}$$

in other words

$$u_i(0, x_1, \cdots, x_i) = 0. \tag{13}$$

Therefore every monomial in u_i contains x_0; let us show that u_i *does not contain* $x_1, \cdots, x_i$. Indeed, suppose $u_i(x) = \sum_{r=0}^{\infty} x_i^r f_r(x_0, \cdots, x_{i-1})$, and suppose h is the smallest value of $r > 0$ for which $f_r \neq 0$; identifying in both sides of (11) the terms in x_i^h gives

$$f_h(x_0, \cdots, x_{i-1}) = f_h(x_0 + y_0, \cdots, \phi_{i-1}(x, y)) + F$$

where F is a polynomial in $x_0, y_0, \cdots, x_{i-1}, y_{i-1}, y_i$, each term of which con-

tains either y_i or an x_k of index $k \leq i-1$ (due to the fact that every monomial in ψ_i contains at least such an x_k). If we replace $x_0, \cdots, x_{i-1}$ by 0 in this identity, we get therefore

$$c_h = f_h(y_0, \cdots, y_{i-1}) + \sum_{k=1}^{\infty} y_i^k g_k(y_0, \cdots, y_{i-1})$$

where c_h is the constant term in f_h, and this shows that f_h is a *constant*. But as we have seen before that each monomial in f_h must contain x_0, we have $f_h = 0$, hence u_j cannot contain x_i. Suppose then that k is the highest index j such that u_i contains x_j, and let again $u_i(\boldsymbol{x}) = \sum_{r=0}^{\infty} x_k^r g_r(x_0, \cdots, x_{k-1})$; suppose $k > 0$, and that h is the smallest value of $r > 0$ for which $g_r \neq 0$. Identifying on both sides of (11) the terms in x_k^h, we see by the same argument as above that $g_h = 0$. Equation (11) reduces therefore to $u_i(x_0 + y_0) = u_i(x_0) + u_i(y_0)$, hence

$$u_i(\boldsymbol{x}) = c_0 x_0 + c_1 x_0^p + \cdots + c_k x_0^{p^k} + \cdots.$$

Let $C_i = (c_i, 0, 0, \cdots)$ in $\mathfrak{W}(K)$, and consider the endomorphism

$$\boldsymbol{v}_i = \boldsymbol{t}^i(C_0 + C_1 \boldsymbol{p} + \cdots + C_j \boldsymbol{p}^j + \cdots). \tag{14}$$

It is clear that the j-th components of $\boldsymbol{u}(\boldsymbol{x})$ and $\boldsymbol{v}_i(\boldsymbol{x})$ are the same for $j \leq i$ (and 0 for $j < i$). The inductive argument can then be carried on in an obvious fashion, and shows that

$$\boldsymbol{u} = \boldsymbol{v}_0 + \boldsymbol{v}_1 + \cdots + \boldsymbol{v}_i + \cdots$$

the infinite sum having a meaning in $\mathcal{E}(K)$. Therefore, we see that we can write $\boldsymbol{u} = \sum_{i,j} \boldsymbol{t}^i C_{ij} \boldsymbol{p}^j$, where $C_{ij} \in \mathfrak{W}(K)$. If we now assume that K is *perfect*, we have

$$\boldsymbol{t}^i C_{ij} \boldsymbol{p}^j = \boldsymbol{t}^{i-j} C_{ij}^{\sigma^{-j}} \boldsymbol{\pi}^j \qquad \text{if } j \leq i$$

$$\boldsymbol{t}^i C_{ij} \boldsymbol{p}^j = C_{ij}^{\sigma^{-i}} \boldsymbol{\pi}^i \boldsymbol{p}^{j-i} \qquad \text{if } j \geq i,$$

from which (using the fact that $\mathfrak{W}(K)$ is complete) it is easy to deduce that $\boldsymbol{u}$ has the form (10).

To prove uniqueness, suppose $\boldsymbol{u}$ is equal to the right-hand side of (10) and is 0; we have to show that all the A_k and B_k are 0. Suppose the contrary, and let us prove first that it is impossible that $\omega(A_k) = 0$ or $\omega(B_k) = 0$ for some k. Indeed, suppose first $\omega(A_k) = 0$ for some $A_k \neq 0$, and let h be the smallest of the indices k having that property; then if $A_h = (a_{h0}, \cdots)$, $a_{h0} \neq 0$ and the component of index 0 of $\boldsymbol{u}(\boldsymbol{x})$ would be $a_{h0} x_0^{p^h} + \cdots$, the terms omitted having degree $> p^h$, contrary to assumption. If on the other hand

$\omega(B_k) = 0$ for some $B_k \neq 0$, let again $h \geq 1$ be the smallest index having that property; then, in the component of $\boldsymbol{u}(\boldsymbol{x})$ of index h, there would be only one term $b_{h0}x_0$ of weight 0, with $b_{h0} \neq 0$, which is again contrary to the assumption $\boldsymbol{u} = 0$. Suppose now we have proved that the minimum value of the $\omega(A_k)$ and $\omega(B_k)$ (for the non zero coefficients) cannot be $< j$, and let us prove it cannot be equal to j. Let us write $A_k = A_k'\boldsymbol{\pi}$, $B_k = B_k'\boldsymbol{\pi}$, where the minimum value of the $\omega(A_k')$ and $\omega(B_k')$ is therefore $j-1$. As $\boldsymbol{\pi} = \boldsymbol{tp}$, and the relation $\boldsymbol{wp} = 0$ implies $\boldsymbol{w} = 0$, we have

$$\sum_{k=1}^{\infty} \boldsymbol{t}^{k+1}B_k'^{\sigma} + \boldsymbol{t}A_0'^{\sigma} + A_1'\boldsymbol{\pi} + \sum_{k=2}^{\infty} A_k'\boldsymbol{\pi}\boldsymbol{p}^{k-1} = 0.$$

This already implies contradiction if $\omega(A_0')$ or one of the $\omega(B_k')$ is $j-1$; if not, we can again divide by $\boldsymbol{p}$ on the right and after a finite number of steps, we reach the desired contradiction.

Theorem 1 is thus completely proved. In what follows, we shall use only the endomorphisms of type

$$B_0 + \boldsymbol{t}B_1 + \cdots + \boldsymbol{t}^k B_k + \cdots \tag{15}$$

which (without any assumption on K) constitute a subring $\mathcal{E}^+(K)$ of $\mathcal{E}(K)$. The preceding argument shows that an endomorphism of $\mathcal{E}^+(K)$ has only one development (15).

5. Abelian groups associated with endomorphisms of $\boldsymbol{H^n}$. There exists a recursive isomorphism $\boldsymbol{h}$ of the additive Witt group W on the hyperexponential group H, such that $h_i(\boldsymbol{x})$ is an isobaric polynomial $x_i + \cdots$ of weight p^i for each $i \geq 0$, $h_0(\boldsymbol{x}) = x_0$, $h_1(\boldsymbol{x}) = x_1$ ([5, no. 7], and [6]). Any K-endomorphism of H (in the same sense as in no. 2) can therefore be written $\boldsymbol{huh}^{-1}$, where $\boldsymbol{u} \in \mathcal{E}(K)$. In what follows, we will identify $\boldsymbol{u}$ and $\boldsymbol{huh}^{-1}$; this will certainly lead to no confusion regarding the endomorphisms $\boldsymbol{t}$ and $\boldsymbol{p}$, for $\boldsymbol{hph}^{-1}$ and $\boldsymbol{hth}^{-1}$ are respectively the Frobenius homomorphism and the shift homomorphism in the group H.

Consider now the endomorphisms of the group H^n, direct product of n groups isomorphic to H; we will denote by $\boldsymbol{x}^{(i)} = (x_0^{(i)}, \cdots, x_h^{(i)}, \cdots)$ $(1 \leq i \leq n)$ the systems of indeterminates corresponding to each of the factors. A recursive endomorphism $\boldsymbol{u}$ of H^n will therefore consist in n systems $\boldsymbol{u}^{(i)} = (u_0^{(i)}, \cdots, u_h^{(i)}, \cdots)$ of power series in the $x_h^{(i)}$ $(1 \leq i \leq n)$, such that $u_h^{(i)}$ contains only the $x_k^{(j)}$ such that $k \leq h$ and $1 \leq j \leq n$). The standard argument determining the endomorphisms of a module which is a direct sum of n isomorphic submodules proves in addition that the endo-

morphisms $\boldsymbol{u}$ correspond, in a one-to-one fashion, to *square matrices* $(\boldsymbol{f}^{(ij)})$ of order n, where the $\boldsymbol{f}^{(ij)}$ $(1\leq i\leq n, 1\leq j\leq n)$ are elements of the ring of endomorphisms of H (identified to $\mathcal{E}(K)$). More precisely, one can write symbolically

$$\boldsymbol{u}^{(i)}(\boldsymbol{x}^{(1)},\cdots,\boldsymbol{x}^{(n)})=\sum_{j=1}^{n}\boldsymbol{f}^{(ij)}(\boldsymbol{x}^{(j)}) \tag{16}$$

the "sum" in the right hand side being understood as taken *for the group law of* H.

From now on until no. 10, $\phi=(\phi_h)_{h=0,1\cdots}$ will always designate the group law of H, so that, with the notations of [5, no. 5], we have

$$\phi_h(x_0,\cdots,x_h;y_0,\cdots,y_h)=x_h+y_h+\sum_{1<k<p^h}E_k(\boldsymbol{x})E_{p^h-k}(\mathbf{y})$$

where E_k is an isobaric polynomial of weight k.

6. With the preceding notations, we now suppose given an endomorphism $\boldsymbol{u}$ of H^n such that the endomorphisms $\boldsymbol{f}^{(ij)}$ of H *belong to the ring* $\mathcal{E}^+(K)$ (no. 4); owing to (16), this implies that in the power series $u_h^{(i)}$, all monomials *have a weight* $\leq p^h$, and in particular the terms containing the indeterminates $x_h^{(j)}$ $(1\leq j\leq n)$ are of the *first* (*total*) *degree*. Generalizing the method introduced in [5, no. 9], we are going to define, with the help of $\boldsymbol{u}$, the *hyperalgebra of an abelian group of dimension* n (over K).

In order to do this, we consider the algebra P of polynomials with respect to n sequences of indeterminates S_{hi} $(1\leq i\leq n, h=0,1,\cdots)$, having coefficients in K, and in this algebra, we consider the ideal $\mathfrak{a}$ generated by the polynomials

$$S_{hi}^{p}-u_h^{(i)}(S_{01},\cdots,S_{0n};\cdots;S_{h1},\cdots,S_{hn}) \tag{17}$$
$$(1\leq i\leq n; h=0,1,\cdots).$$

For each index $\alpha=(\alpha_1,\cdots,\alpha_n)$ (α_i integers ≥ 0), let

$$E_\alpha(S_{01},\cdots,S_{h1},\cdots;S_{02},\cdots,S_{h2},\cdots;\cdots;S_{0n},\cdots,S_{hn},\cdots)$$
$$=E_{\alpha_1}(S_{01},\cdots,S_{h1},\cdots)E_{\alpha_2}(S_{02},\cdots,S_{h2},\cdots)\cdots E_{\alpha_n}(S_{0n},\cdots,S_{hn},\cdots).$$

Let X_{hi} be the class of S_{hi} in the quotient algebra $P/\mathfrak{a}$, and

$$Z_\alpha=E_\alpha(X_{01},\cdots,X_{h1},\cdots;\cdots;X_{0n},\cdots,X_{hn},\cdots). \tag{18}$$

THEOREM 2. *The elements* Z_α *form a basis of the algebra* $P/\mathfrak{a}$, *such that, with this basis,* $P/\mathfrak{a}$ *is the hyperalgebra of an abelian group* G *of dimension* n.

It is clear that the algebra $P/\mathfrak{a}$ is generated by the X_{hi}, and more precisely, from the relations

$$X_{hi}^{p} = u_h^{(i)}(X_{01}, \cdots, X_{0n}; \cdots; X_{h1}, \cdots, X_{hn}) \tag{19}$$

it follows, by an easy inductive argument on h, that the elements of $P/\mathfrak{a}$ are linear combinations of monomials X_α in the X_{hi} where the exponent of each X_{hi} is $< p$; moreover, relations (19) also show that the linear combinations of the X_α of height $h(\alpha) < r$ constitute a subalgebra $\mathfrak{F}_r$ of $P/\mathfrak{a}$. From the definition (18), it follows that the Z_α belong to $\mathfrak{F}_r$ for $h(\alpha) < r$; we are going to prove that the Z_α of height $h(\alpha) < r$ constitute a *basis* of $\mathfrak{F}_r$; the family (Z_α) (without restriction on α) will then of course constitute a basis of $P/\mathfrak{a}$.

The first step consists in proving that the

$$X_\alpha = X_{01}^{\nu_{01}} \cdots X_{0n}^{\nu_{0n}} X_{11}^{\nu_{11}} \cdots X_{1n}^{\nu_{1n}} \cdots X_{h1}^{\nu_{h1}} \cdots X_{hn}^{\nu_{hn}}$$

(where $\alpha_i = \sum_{k=0}^{h} \nu_{ki} p^k$ is the p-adic development of α_i, and $h < r$) constitute a basis for $\mathfrak{F}_r$. This will be proved by induction on r, as a consequence of the fact that all the monomials, in the polynomial $u_h^{(i)}$, have a weight $\leq p^h$, and of the elementary lemma:

LEMMA 1. *Let A be a commutative ring with unit element, and let $\mathfrak{b}$ be the ideal in the ring of polynomials $A[Y_1, \cdots, Y_n]$, generated by the polynomials*

$$Q_i = Y_i^m - \sum_{j=1}^{n} b_{ij} Y_j - c_i \qquad (1 \leq i \leq n)$$

m being an integer > 1, the b_{ij} and c_i elements of A. Then if $\bar{Y}_i$ is the class of $Y_i \bmod \mathfrak{b}$, the monomials $\bar{Y}_1^{\mu_1} \bar{Y}_2^{\mu_2} \cdots \bar{Y}_n^{\mu_n}$ with $0 \leq \mu_i < m$, constitute a basis of the quotient ring $A[Y_1, \cdots, Y_n]/\mathfrak{b}$ over the ring A.

To prove the lemma, let us assign weight 1 to the Y_i, weight m to each polynomial Q_i. Then it is readily seen by induction on k that every monomial in $Y_1, \cdots, Y_n$, of total degree $\leq k$, can be expressed as a linear combination of monomials in $Y_1, \cdots, Y_n, Q_1, \cdots, Q_n$, of total weight $\leq k$, the exponent of each Y_i in these monomials being $< m$. As the number of these last monomials of total weight $\leq k$ is exactly equal to the number of monomials in $Y_1, \cdots, Y_n$ of total degree $\leq k$, they constitute a basis for the set of polynomials in $Y_1, \cdots, Y_n$ of total degree $\leq k$; the lemma follows immediately from this result.

The fact that the X_α with $h(\alpha) < r$ constitute a basis for $\mathfrak{F}_r$ is then proved by applying the lemma in succession to $A = K$, $A = \mathfrak{F}_1, \cdots, A = \mathfrak{F}_{r-1}$.

7. Next we remark (see [5, no. 8]) that if $k = v_0 + v_1 p + \cdots + v_h p^h$ (p-adic development, $v_h > 0$), there is in $E_k(x_0, \cdots, x_h)$ the monomial $\frac{x_0^{v_0} x_1^{v_1} \cdots x_h^{v_h}}{v_0! v_1! \cdots v_h!}$; moreover, if we order the monomials in $x_0, \cdots, x_h$ in the *inverse* lexicographic order, the preceding monomial is the "first" in E_k. Let us next order the S_{hi} in a linear sequence:

$$S_{01}, \cdots, S_{0n}, S_{11}, \cdots, S_{1n}, \cdots, S_{h1}, \cdots, S_{hn}, \cdots.$$

If we put $\alpha_i = \sum_l v_{li} p^l$ (p-adic development), the preceding remark shows that if we order the monomials in the S_{hi} in the inverse lexicographic order, the "first" monomial in E_α is the monomial $\frac{1}{\alpha!} S_\alpha$ (with notation similar to that of the X_α). Consider now the expression of Z_α as a linear combination of the monomials X_λ, and let us order these monomials in the same order as the corresponding monomials in the S_{hi}. We observe that if in a monomial $S_{01}^{\mu_{01}} \cdots S_{hn}^{\mu_{hn}}$ in E_α there is an exponent $\mu_{kj} \geq p$, then there must be an index $l > k$ such that we will have $\mu_{lj} < v_{lj}$, owing to the fact that the E_k are *isobaric*; considering the *largest* index k for which there is a j such that $\mu_{kj} \geq p$, we see therefore that in the expression of the corresponding monomial $X_{01}^{\mu_{01}} \cdots X_{hn}^{\mu_{hn}}$ as a linear combination of the X_λ, every monomial X_λ is *after* the monomial $\frac{1}{\alpha!} X_\alpha$ (which itself comes from the replacement of the S_{hi} by the X_{hi} in $\frac{1}{\alpha!} S_\alpha$), due to relations (19). In other words, in the expression of Z_α as a linear combination of the X_λ, the "first" term is $\frac{1}{\alpha!} X_\alpha$. From the linear independence of the X_α, it follows at once that the Z_α are linearly independent over K.

This result ends our proof of the fact that the Z_α with $h(\alpha) < r$ constitute a basis for $\mathfrak{g}_r$, for their number is the same as that of the X_α with $h(\alpha) < r$.

8. We can now write

$$Z_\alpha Z_\beta = \sum_\gamma d_{\alpha\beta\gamma} Z_\gamma \qquad (d_{\alpha\beta\gamma} \in K) \tag{20}$$

and by definition, these relations can be interpreted as polynomial congruences

$$E_\alpha E_\beta \equiv \sum_\gamma d_{\alpha\beta\gamma} E_\gamma \pmod{\mathfrak{a}} \tag{21}$$

in the ring P. To prove Theorem 2, we apply the existence theorem [5, Prop. 1]; replace in P and in the polynomials (17) the indeterminates S_{hi}

by new indeterminates T_{hi}, obtaining thus a ring P_1 of polynomials and an ideal $\mathfrak{a}_1$ in P_1, and let Y_{hi} be the class of $T_{hi} \bmod \mathfrak{a}_1$. We then form the elements

$$Z_\alpha{}^0 = \sum_{0 \leq \beta \leq \alpha} E_\beta(X_{01}, \cdots, X_{hn}, \cdots) E_{\alpha-\beta}(Y_{01}, \cdots, Y_{hn}, \cdots)$$

and we have to prove that these elements satisfy the *same* relations (20) as the Z_α. But from the expression of the ϕ_h in terms of the E_k and the definition of the hyperexponential series, it follows that we have [5, no. 8]

$$Z_\alpha{}^0 = E_\alpha(\Phi_{01}, \cdots, \Phi_{h1}, \cdots; \cdots; \Phi_{0n}, \cdots, \Phi_{hn}, \cdots) \tag{22}$$

where

$$\Phi_{hi} = \phi_h(X_{0i}, Y_{0i}, X_{1i}, Y_{1i}, \cdots, X_{hi}, Y_{hi}).$$

Now, if in the polynomial congruences (21) we replace each S_{hi} by Φ_{hi}, we see that the difference

$$Z_\alpha{}^0 Z_\beta{}^0 - \sum_\gamma d_{\alpha\beta\gamma} Z_\gamma{}^0$$

is a linear combination (with coefficients which are polynomials in the Φ_{hi}, and therefore in the X_{hi} and Y_{hi}) of the polynomials

$$\Phi_{hi}{}^p - u_h{}^{(i)}(\Phi_{01}, \cdots, \Phi_{0n}; \cdots; \Phi_{h1}, \cdots, \Phi_{hn}) \tag{23}$$

and therefore our proof will be ended if we establish that the expressions (23) all vanish. But as the ϕ_h have their coefficients in the prime field $\boldsymbol{F}_p$, we have

$$\Phi_{hi}{}^p = \phi_h(X_{0i}{}^p, Y_{0i}{}^p, \cdots, X_{hi}{}^p, Y_{hi}{}^p)$$

and if we equal the expression (23) to 0, we obtain the relation

$$\begin{aligned}\phi_h(X_{0i}{}^p, Y_{0i}{}^p, \cdots, X_{hi}{}^p, Y_{hi}{}^p) \\ = u_h{}^{(i)}(\phi_0(X_{01}, Y_{01}), \cdots, \phi_0(X_{0n}, Y_{0n}); \cdots; \\ \cdots; \phi_h(X_{01}, \cdots, Y_{h1}), \cdots, \phi_h(X_{0n}, \cdots, Y_{hn})).\end{aligned}$$

But if we replace the $X_{hi}{}^p$ by their expressions (19), and the $Y_{hi}{}^p$ by the corresponding expressions, the relations we obtain follow from the assumption that $\boldsymbol{u}$ is an *endomorphism* of the group H^n. The proof of Theorem 2 is thus complete.

9. We will say that the abelian group G, the existence of which follows from Theorem 2, is *associated* to the endomorphism $\boldsymbol{u}$ of H^n. Our proof gives an "explicit" determination of that group when $\boldsymbol{u}$ is known; more precisely, the translation operator in G is given by

$$R_{\boldsymbol{y}} = \prod_{i=1}^{n} Hex(y_i X_{0i}, y_i{}^p X_{1i}, \cdots, y_i{}^{p^k} X_{hi}, \cdots)$$

where in the development of the right-hand side, the powers of the X_{hi} must be reduced to exponents $< p$ according to the relations (19). Moreover, the algebra P can be identified with the hyperalgebra of the product U^n of n groups isomorphic with the "universal group" U [5, no. 8], the S_{hi} being the invariant semi-derivations which generate that hyperalgebra; the proof of Theorem 2 shows then [5, Prop. 2] that the natural mapping of P onto $P/\mathfrak{a}$ is the derived homomorphism $\boldsymbol{v}'$ of a homomorphism $\boldsymbol{v}$ of U^n onto G.

10. Some examples. It is easy to reformulate in terms of matrices (with elements in $\mathcal{E}^+(K)$) the definitions of the particular groups considered in [4] and [5]. For instance, to the null matrix (of order n) corresponds the direct product $W_1{}^n$ of n additive groups; to the unit matrix, the direct product $(W_1{}^*)^n$ of n multiplicative groups. The group $G_{n,m,r}$ defined in [5, no. 9] corresponds to the matrix

$$\begin{pmatrix} 0 & I & 0 & & \cdots & 0 \\ 0 & 0 & I & & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & & \cdots & I \\ 0 & \cdots & & \boldsymbol{t}^r & \cdots & 0 \end{pmatrix}$$

where in the last row, the element $\boldsymbol{t}^r$ is in the $(m+1)$-st column.

Similarly, the "streak", "tree" and "braid" types of groups of dimension 2 defined in [5, no. 10], correspond respectively to the matrices

$$\begin{pmatrix} 0 & \boldsymbol{t}^r \\ 0 & 0 \end{pmatrix}, \qquad \begin{pmatrix} 0 & \boldsymbol{t}^r \\ 0 & \boldsymbol{t}^s \end{pmatrix}, \qquad \begin{pmatrix} 0 & \boldsymbol{t}^r \\ \boldsymbol{t}^s & 0 \end{pmatrix}.$$

11. The structure of abelian formal Lie groups. The construction of abelian Lie groups given by Theorem 2 is in fact general enough to give *all* abelian Lie groups, up to an isomorphism; in other words:

THEOREM 3. *Every abelian formal Lie group G of dimension n over a field K is isomorphic to an abelian group associated to an endomorphism of H^n.*

We start by remarking that the invariant derivations X_{0i} $(1 \leq i \leq n)$ of G satisfy relations of the form

$$X_{0i}{}^p = \sum_{j=1}^{n} a_{ij} X_{0j} \qquad (1 \leq i \leq n, a_{ij} \in K).$$

We consider the Witt vectors $A_{ij} = (a_{ij}, 0, 0, \cdots)$, and the endomorphism $\boldsymbol{u}^{(0)}$ of H^n defined by the matrix (A_{ij}) (whose elements are identified with endomorphisms of H, as explained in no. 5). Let $L^{(0)}$ be the abelian group asso-

ciated to $\boldsymbol{u}^{(0)}$; then the invariant derivations X'_{0i} $(1 \leq i \leq n)$ of $L^{(0)}$ satisfy the same relations

$$X'_{0i}{}^{p} = \sum_{j=1}^{n} a_{ij} X'_{0j} \qquad (1 \leq i \leq n)$$

(cf. relations (19)).

As a basis for an inductive argument, we will next suppose that there is an abelian group $L^{(r)}$, associated with an endomorphism $\boldsymbol{u}^{(r)}$ of H^n, such that, if we denote by X_{hi} (resp. X'_{hi}) the generating invariant semi-derivations in the hyperalgebra of G (resp. $L^{(r)}$), the following properties hold:

1. if Z_α (resp. Z'_α) is the coefficient of y_α in the translation operator of G (resp. $L^{(r)}$), and if $Z_\alpha = \sum_\lambda e_{\alpha\lambda} X_\lambda$ $(e_{\alpha\lambda} \in K)$, then, for all indices α of height $h(\alpha) < r$, we have $Z'_\alpha = \sum_\lambda e_{\alpha\lambda} X'_\lambda$;

2. the multiplication tables of the subalgebras $\mathfrak{g}_r$, $\mathfrak{g}'_r$ of the hyperalgebras of G and $L^{(r)}$ are identical; in other words, if $Z_\alpha Z_\beta = \sum_\gamma d_{\alpha\beta\gamma} Z_\gamma$, we have $Z'_\alpha Z'_\beta = \sum_\gamma d_{\alpha\beta\gamma} Z'_\gamma$ for $h(\alpha) < r$ and $h(\beta) < r$;

3. if we have

$$X_{ri}{}^{p} = \sum_{j=1}^{n} a_{ij}{}^{p^r} X_{rj} + \sum_\lambda b_{i\lambda} Z_\lambda \qquad (1 \leq i \leq n)$$

then also

$$X'_{ri}{}^{p} = \sum_{j=1}^{n} a_{ij}{}^{p^r} X'_{rj} + \sum_\lambda b_{i\lambda} Z'_\lambda$$

(the sum extended over indices λ of height $h(\lambda) < r$).

Let $(\phi_i)_{1 \leq i \leq n}$ and $(\phi'_i)_{1 \leq i \leq n}$ be the series defining the group laws of G and $L^{(r)}$ respectively; it follows from assumption 2. that for $h(\alpha) < r$ and $h(\beta) < r$, the coefficients of $x_\alpha y_\beta$ in ϕ_i and in ϕ'_i are the *same* [4, formula (5)]. Let $\boldsymbol{v}$ (resp. $\boldsymbol{w}$) be the isomorphism of G (resp. $L^{(r)}$) on a group $\bar{G}$ (resp. $\bar{L}^{(r)}$) obtained by the standard process described in [2] (see also [4, no. 4]), such that the group laws of $\bar{G}$ and $\bar{L}^{(r)}$ are *canonical*; we have $v_i(\boldsymbol{x}) = x_i + \cdots$ (resp. $w_i(\boldsymbol{x}) = x_i + \cdots$) for every i, the unwritten terms having total degree ≥ 2. Moreover, the description of the standard process given in [2], and the fundamental fact that (with the notations of [1]) no power series $P_\alpha(\boldsymbol{x})$ except the $P_{p^r \epsilon_i}$ can contain monomials in $x_j{}^{p^r}$ [1, formula (34)], show (together with the preceding remarks) that the coefficients of x_α, for $h(\alpha) < r$, as well as the coefficients of the monomials $x_j{}^{p^r}$, are the *same* in v_i and w_i $(1 \leq i \leq n)$. It is then clear that properties 1. and 2. still hold when G and $L^{(r)}$ are respectively replaced by $\bar{G}$ and $\bar{L}^{(r)}$; but 3. also holds, for we have

$\boldsymbol{v}'(X_{ri}) = \bar{X}_{ri} + \sum_\lambda g_{i\lambda}\bar{X}_\lambda$ and $\boldsymbol{w}'(X'_{ri}) = \bar{X}'_{ri} + \sum_\lambda g_{i\lambda}\bar{X}'_\lambda$ with the *same* coefficients (summation over the indices of height $h(\lambda) < r$), as follows from the preceding argument.

Now we apply the uniqueness theorem [2, Th. 2], or rather the corresponding result which is obtained by "cutting down" the power series "modulo the monomials $x_i^{p^{r+1}}$", and which obviously follows from the proof of the uniqueness theorem (see [4, no. 4]): as the "constants of structure" $c_{\alpha\beta\gamma}$ in the algebras $\bar{\mathfrak{s}}_{r+1}$ and $\bar{\mathfrak{s}}'_{r+1}$ are the *same*, the fact that the group laws of $\bar{G}$ and $\bar{L}^{(r)}$ are canonical implies that properties 1. and 2. are valid for $\bar{G}$ and $\bar{L}^{(r)}$ *when the conditions* $h(\alpha) < r$, $h(\beta) < r$ *are replaced by* $h(\alpha) < r+1$ *and* $h(\beta) < r+1$.

This is of course still true if we apply to *both* $\bar{G}$ and $\bar{L}^{(r)}$ the isomorphism $\boldsymbol{w}^{-1}$. In other words, if we replace G by the group which is the image of G under the isomorphism $\boldsymbol{q}^{(r)} = \boldsymbol{w}^{-1}\boldsymbol{v}$, conditions 1. and 2. are now satisfied when in the inequalities on the heights, r *is replaced by* $r+1$; and of course, condition 3. holds without change.

For future use, we remark here that the series $q_i^{(r)}(\boldsymbol{x}) = x_i + \cdots$ $(1 \leq i \leq n)$, where the unwritten terms are *of total degree* $\geq p^r$; this follows from the identity of the terms of total degree $< p^r$ in v_i and w_i.

12. Suppose now that the expression of $X'^{p}_{r+1,i}$ in the hyperalgebra of $L^{(r)}$ is

$$X'^{p}_{r+1,i} = \sum_{j=1}^{n} a_{ij}{}^{p^{r+1}} X'_{r+1,j} + \sum_\mu b'_{i\mu} Z'_\mu \qquad (1 \leq i \leq n) \tag{24}$$

where, in the summation, the indices μ are such that $h(\mu) < r+1$. We want to prove that the differences

$$Y_i = X^{p}_{r+1,i} - \sum_{j=1}^{n} a_{ij}{}^{p^{r+1}} X_{r+1,j} - \sum_\mu b'_{i\mu} Z_\mu \qquad (1 \leq i \leq n)$$

are *derivations*. To do this, we remark [4, Lemma 2] that we have

$$X'^{p}_{r+1,i}(fg) = f \cdot X'^{p}_{r+1,i} g + g \cdot X'^{p}_{r+1,i} f + \sum_{0<k<p^{r+1}} (Z'^{p}_{k\varepsilon_i} f)\,(Z'^{p}_{(p^{r+1}-k)\varepsilon_i} g). \tag{25}$$

On the other hand, we can write

$$Z'^{p}_{k\varepsilon_i} = \sum_\rho g_{ik\rho} Z'_\rho \qquad (1 \leq i \leq n, 0 < k < p^{r+1}) \tag{26}$$

where the summation extends over indices $\rho \neq 0$ of height $< r+1$. Replacing in (25) and comparing with (24), we see that, for $|\mu| > 1$

$$b'_{i\mu} = \sum_k g_{ik\rho} g_{i,p^{r+1}-k,\mu-\rho} \tag{27}$$

and

$$a_{ij}{}^{p^{r+1}} = \sum_k g_{i,k,l\epsilon_j} g_{i,p^{r+1}-k,(p^{r+1}-l)\epsilon_j}$$

for any ρ such that $0 < \rho < \mu$ and any l such that $0 < l < p^{r+1}$; in other words, the $b'_{i\mu}$ for $|\mu| > 1$ are entirely determined by the $g_{ik\rho}$. But from our assumptions it follows that we also have

$$Z_{k\epsilon_i}{}^p = \sum_\rho g_{ik\rho} Z_\rho \qquad (1 \leq i \leq n, 0 < k < p^{r+1}) \tag{28}$$

with the *same* coefficients. On the other hand, we have by [4, Lemma 2]

$$X_{r+1,i}{}^p(fg) = f \cdot X_{r+1,i}{}^p g + g \cdot X_{r+1,i}{}^p f + \sum_{0<k<p^{r+1}} (Z_{k\epsilon_i}{}^p f)(Z_{(p^{r+1}-k)\epsilon_i}{}^p g). \tag{29}$$

Replacing the $Z_{k\epsilon_i}{}^p$ by their expressions (28), and using relations (27), we see that in the expression of $Y_i(fg)$ as a sum $\sum_{\lambda,\mu} h_{\lambda\mu}(Z_\lambda f)(Z_\mu g)$, there is no term in which *both* λ and μ are $\neq 0$ and this proves our assertion.

13. We can therefore write

$$Y_i = \sum_{j=1}^n a_{ij}{}^{(r+1)} X_{0j} \qquad (1 \leq i \leq n, a_{ij}{}^{(r+1)} \in K).$$

Suppose the endomorphism $\boldsymbol{u}^{(r)}$ of H^n corresponded to the matrix $(\boldsymbol{f}^{(i,j,r)})$, where $\boldsymbol{f}^{(i,j,r)}$ belongs to $\mathcal{E}^+(K)$. Consider the Witt vectors $A_{ij}{}^{(r+1)} = (a_{ij}{}^{(r+1)}, 0, 0, \cdots)$, and the matrix

$$(\boldsymbol{f}^{(i,j,r+1)}) = (\boldsymbol{f}^{(i,j,r)} + \boldsymbol{t}^{r+1} A_{ij}{}^{(r+1)})_{1 \leq i,j \leq n}. \tag{30}$$

This matrix corresponds to an endomorphism $\boldsymbol{u}^{(r+1)}$ of H^n, to which in turn correspond an abelian group $L^{(r+1)}$; if we recall the definition of $L^{(r+1)}$ by means of relations (19), we see that we have finally reached the following conclusion: the image of G under the isomorphism $\boldsymbol{q}^{(r)}$, and the group $L^{(r+1)}$, satisfy conditions 1., 2., 3. *where r has been replaced by $r+1$.*

It is now easy to bring our inductive argument to a close. From the last remark of no. 11, it follows that the "infinite product $\cdots \boldsymbol{q}^{(r)} \cdots \boldsymbol{q}^{(1)} \boldsymbol{q}^{(0)}$ is meaningful and represents an isomorphism of G on a group $\bar{G}$. On the other hand, formulae (30) show that the matrices $(\boldsymbol{f}^{(i,j,r)})$ "converge" to a matrix $(\boldsymbol{f}^{(ij)})$ with elements in $\mathcal{E}^+(K)$, corresponding to an endomorphism $\boldsymbol{u}$ of H^n. If $\bar{L}$ is then the abelian group defined by that endomorphism, our construction is such that the constants $d_{\alpha\beta\gamma}$ in the hyperalgebras of $\bar{G}$ and $\bar{L}$ are the *same*, and therefore these two groups are *identical*, which concludes the proof of Theorem 3.

We add two remarks: the first is that, forming (according to Theorem 2) abelian groups corresponding to endomorphisms of H^n, we can always limit ourselves to the case in which the matrix $(\boldsymbol{f}^{(ij)})$ is such that, if $\boldsymbol{f}^{(ij)} = \sum_{k=0}^{\infty} \boldsymbol{t}^k A_{ij}^{(k)}$, the Witt vectors $A_{ij}^{(k)}$ which are $\neq 0$ are such that $\omega(A_{ij}^{(k)}) = 0$; this follows from (30).

On the other hand, Theorems 2 and 3 yield, for abelian groups, the following result, which is analogous to the well-known theorem in classical Lie theory, asserting that one-parameter subgroups "fill up" the group locally: for any element $X = \sum_{i=1}^{n} \xi_i X_{0i} \neq 0$ $(\xi_i \in K)$ of the Lie algebra $\mathfrak{g}_0$ of an abelian group G, there exists a homomorphism $\boldsymbol{u}$ of the hyperexponential group H into G such that $\boldsymbol{u}'(S_{00}) = X$ (S_{hi} being the usual generators of the Lie hyperalgebra of H, noted X_{hi} in [5, no. 5]). One has merely to make a linear transformation on the indeterminates in G, which transforms X into X_{00}, for instance; we have then a homomorphism of U^n onto G (no. 9), and the restriction of that homomorphism to the first factor of the product, composed with an isomorphism of H onto U, satisfies the required conditions. It would be very interesting to know if this result extends to non-abelian formal Lie groups.

14. Homomorphisms of abelian groups. It follows from theorem 3 that the study of abelian formal Lie groups can be reduced to that of the groups associated with endomorphisms of groups H^n; we are going to study the homomorphisms of such groups.

Let G and $\bar{G}$ be two such groups, of respective dimensions n and m, and suppose they are respectively associated with an endomorphism $\boldsymbol{u}$ of H^n and an endomorphism $\boldsymbol{v}$ of H^m; $\boldsymbol{u}$ and $\boldsymbol{v}$ can respectively be represented by square matrices $\boldsymbol{U} = (\boldsymbol{f}^{(ij)})$ and $\boldsymbol{V} = (\boldsymbol{g}^{(ij)})$ of order n and m respectively, having their elements in the ring $\mathcal{E}^+(K)$. We shall designate by P and Q the algebras of polynomials, by $\mathfrak{a}$ and $\mathfrak{b}$ the ideals in these algebras determined respectively by $\boldsymbol{u}$ and $\boldsymbol{v}$, so that the hyperalgebras of G and $\bar{G}$ are respectively isomorphic to $P/\mathfrak{a}$ and $Q/\mathfrak{b}$ (no. 6); S_{hi} and T_{hi} will be the indeterminates in P and Q respectively, X_{hi} and Y_{hi} their classes mod. $\mathfrak{a}$ and mod. $\mathfrak{b}$ respectively.

We will first consider the following question. Let $\boldsymbol{w} = (\boldsymbol{w}^{(i)})_{1 \leq i \leq n}$ be a homomorphism of H^m into H^n, $\boldsymbol{w}^{(i)} = (w_0^{(i)}, \cdots, w_h^{(i)}, \cdots)$ being n systems of power series in the $x_h^{(j)}$ $(1 \leq j \leq m)$ such that $w_h^{(i)}$ contains only the $x_k^{(j)}$ such that $k \leq h$. To this homomorphism is again associated an $n \times m$

matrix $\boldsymbol{W} = (\boldsymbol{h}^{(ij)})$ $(1 \leq i \leq n, 1 \leq j \leq m)$ with elements $\boldsymbol{h}^{(ij)}$ in $\mathcal{E}(K)$, such that (with the same conventions as in no. 5)

$$\boldsymbol{w}^{(i)}(\boldsymbol{x}^{(1)}, \cdots, \boldsymbol{x}^{(m)}) = \sum_{j=1}^{m} \boldsymbol{h}^{(ij)}(\boldsymbol{x}^{(j)}) \qquad (1 \leq i \leq n).$$

We will always suppose, in addition, that the $\boldsymbol{h}^{(ij)}$ belong to $\mathcal{E}^+(K)$ (which insures that the $w_h^{(i)}$ are in fact polynomials).

We now ask under which conditions on $\boldsymbol{W}$ the formulae

$$\boldsymbol{s}'(X_{hi}) = w_h^{(i)}(Y_{01}, \cdots, Y_{0m}; \cdots; Y_{h1}, \cdots, Y_{hm}) \qquad (1 \leq i \leq n; h = 0, 1, \cdots) \tag{31}$$

define the derivative $\boldsymbol{s}'$ of a *homomorphism* of G into $\bar{G}$.

THEOREM 4. *Suppose K is a perfect field. In order that formulae* (31) *define a homomorphism $\boldsymbol{s}$ of G into $\bar{G}$, it is necessary and sufficient that there exist an $n \times m$ matrix $\boldsymbol{L}$ with elements in $\mathcal{E}^+(K)$, such that*

$$\boldsymbol{U}\boldsymbol{W} - \boldsymbol{W}^{\sigma}\boldsymbol{V} = \boldsymbol{L}(\boldsymbol{\pi} \cdot \boldsymbol{I} - \boldsymbol{t} \cdot \boldsymbol{V}) \tag{32}$$

($\boldsymbol{I}$ being the $m \times m$ unit matrix, and $\boldsymbol{W}^{\sigma}$ being the matrix $((\boldsymbol{h}^{(ij)})^{\sigma})$ the isomorphism σ being defined by $\boldsymbol{a}^{\sigma} = A_0^{\sigma} + \boldsymbol{t}A_1^{\sigma} + \cdots + \boldsymbol{t}^k A_k^{\sigma} + \cdots$ if $\boldsymbol{a} = A_0 + \boldsymbol{t}A_1 + \cdots + \boldsymbol{t}^k A_k + \cdots$).

15. The system of polynomials

$$w_h^{(i)}(T_{01}, \cdots, T_{0m}; \cdots; T_{h1}, \cdots, T_{hm})$$

can be represented by the "one-column matrix" $\boldsymbol{W} \cdot \boldsymbol{x}$, the indeterminates $x_h^{(i)}$ being replaced by T_{hi}. If there is a homomorphism $\boldsymbol{s}$ verifying (31), we must have

$$\boldsymbol{s}'(X_{hi^p}) = (w_h^{(i)})^{\sigma}(Y_{01^p}, \cdots, Y_{0m^p}; \cdots; Y_{h1^p}, \cdots, Y_{hm^p}) \tag{33}$$

$(w_h^{(i)})^{\sigma}$ being the polynomial obtained by raising all the coefficients of $w_h^{(i)}$ to the power p. But considering the definition of $\bar{G}$ by means of the matrix $\boldsymbol{V}$ (no. 6), we see that the right hand sides of (33) are obtained by replacing T_{hj} by Y_{hj} in the system of polynomials represented by the one-column matrix $(\boldsymbol{W}^{\sigma}\boldsymbol{V}) \cdot \boldsymbol{x}$. On the other hand, the definition of G by means of $\boldsymbol{U}$ and formulae (31) show that (if $\boldsymbol{s}$ exists) the left hand sides of (33) are obtained by replacing T_{hj} by Y_{hj} in the system of polynomials represented by the one-column matrix $(\boldsymbol{U}\boldsymbol{W}) \cdot \boldsymbol{x}$. Therefore, a necessary condition is that the matrix $\boldsymbol{C} = \boldsymbol{U}\boldsymbol{W} - \boldsymbol{W}^{\sigma}\boldsymbol{V}$ be such that, when each T_{hj} is replaced by Y_{hj} in the system of polynomials represented by the one-column matrix $\boldsymbol{C} \cdot \boldsymbol{x}$, the

expressions obtained all vanish. This can also be expressed in the following way: the polynomials of the system represented by $\boldsymbol{C} \cdot \boldsymbol{x}$ must *belong to the ideal* $\mathfrak{b}$.

This is certainly the case if $\boldsymbol{C} = \boldsymbol{L}(\boldsymbol{\pi} \cdot \boldsymbol{I} - \boldsymbol{t} \cdot \boldsymbol{V})$, for $\boldsymbol{\pi} \cdot \boldsymbol{I} - \boldsymbol{t} \cdot \boldsymbol{V} = \boldsymbol{t}(\boldsymbol{p} \cdot \boldsymbol{I} - \boldsymbol{V})$ (from (3)), and relations (19) (or rather the corresponding relations for $\bar{G}$) show that the polynomials of the system represented by $(\boldsymbol{p} \cdot \boldsymbol{I} - \boldsymbol{V}) \cdot \boldsymbol{x}$ belong to $\mathfrak{b}$; moreover, if $\boldsymbol{y}$ is a one-column matrix representing a system of polynomials of $\mathfrak{b}$, $\boldsymbol{M} \cdot \boldsymbol{y}$ is also such a matrix, for an arbitrary $n \times m$ matrix $\boldsymbol{M}$ with elements in $\mathfrak{E}^+(K)$. Let us now prove the converse; we can write $\boldsymbol{C} = \Gamma_0 + \boldsymbol{t}\Gamma_1 + \cdots + \boldsymbol{t}^k\Gamma_k + \cdots$, where $\Gamma_k = (C_k^{(ij)})$ is an $n \times m$ matrix with elements in the ring $\mathfrak{W}(K)$ of the Witt-vectors. If we denote by $c_k^{(i)}(T_{01}, \cdots, T_{hm})$ the polynomials of the system represented by $\boldsymbol{C} \cdot \boldsymbol{x}$, and if $C_k^{(ij)} = (c_{k0}^{(ij)}, c_{k1}^{(ij)}, \cdots)$ $(c_{kh}^{(ij)} \in K)$, we have

$$c_0^{(i)}(T_{01}, \cdots, T_{0m}) = \sum_{j=1}^{m} c_{00}^{(ij)} T_{0j}.$$

Now we have seen in the proof of Theorem 2 (no. 6) that such a polynomial cannot belong to $\mathfrak{b}$ unless all the $c_{00}^{(ij)} = 0$; but, as K is perfect, this means that there is a matrix Λ_0 with elements in $\mathfrak{W}(K)$, such that $\Gamma_0 = \Lambda_0 \boldsymbol{\pi}$. We can therefore write $\boldsymbol{C} = \Lambda_0(\boldsymbol{\pi} \cdot \boldsymbol{I} - \boldsymbol{t} \cdot \boldsymbol{V}) + \boldsymbol{t} \cdot \boldsymbol{C}_1$, and $(\boldsymbol{t} \cdot \boldsymbol{C}_1) \cdot \boldsymbol{x}$ must belong to the ideal $\mathfrak{b}$; in other words, we are reduced to the case in which $\Gamma_0 = 0$. More generally, suppose Γ_k is the first coefficient in $\boldsymbol{C}$ which is $\neq 0$; we then have

$$c_k^{(i)}(T_{01}, \cdots, T_{0m}; \cdots; T_{k1}, \cdots, T_{km}) = \sum_{j=1}^{m} c_{k0}^{(ij)} T_{0j}$$

and the same argument as before shows that all the elements $c_{k0}^{(ij)}$ must be 0. By an easy inductive argument, it follows that $\boldsymbol{C} = \boldsymbol{L}(\boldsymbol{\pi} \cdot \boldsymbol{I} - \boldsymbol{t} \cdot \boldsymbol{V})$ with $\boldsymbol{L} = \Lambda_0 + \boldsymbol{t}\Lambda_1 + \cdots + \boldsymbol{t}^k\Lambda_k + \cdots$, the Λ_k being $n \times m$ matrices with elements in $\mathfrak{W}(K)$. This concludes the proof of the *necessity* of condition (32).

16. To prove that the condition is *sufficient*, we consider the homomorphism $\boldsymbol{r}$ of the algebra of polynomials P into the algebra of polynomials Q, defined by

$$\boldsymbol{r}(S_{hi}) = w_h^{(i)}(T_{01}, \cdots, T_{0m}; \cdots; T_{h1}, \cdots, T_{hm}) \qquad (1 \leq i \leq n; h = 0, 1, \cdots) \tag{34}$$

Condition (32) insures that the image of the ideal $\mathfrak{a}$ under the homomorphism $\boldsymbol{r}$ is contained in $\mathfrak{b}$; hence $\boldsymbol{r}$ defines a homomorphism $\boldsymbol{s}'$ of $P/\mathfrak{a}$ into $Q/\mathfrak{b}$, satisfying (31). It remains to be seen that this homomorphism

is the derived homomorphism of a homomorphism $\boldsymbol{s}$ of G into $\bar{G}$; this will be done by showing that the conditions of [5, Prop. 2] are satisfied.

Introducing new sequences of indeterminates S'_{hi}, T'_{hi}, and using the notations of no. 6, we first remark that, as $\boldsymbol{r}$ is a homomorphism of P into Q, the image by $\boldsymbol{r}\otimes\boldsymbol{r}$ of the element

$$\sum_{0\leq\beta\leq\alpha} E_\beta(S_{01},\cdots,S_{hn},\cdots)E_{\alpha-\beta}(S'_{01},\cdots,S'_{hn},\cdots)$$

is obtained by replacing in that expression each S_{hi} (resp. S'_{hi}) by its value $\boldsymbol{r}(S_{hi})$ (resp. $\boldsymbol{r}(S'_{hi})$) given by (34). But from the fact that $\boldsymbol{w}$ is a homomorphism and the arguments in no. 8, it follows that we obtain in that way the expression

$$E_\alpha(\Psi_{01},\cdots,\Psi_{h1},\cdots;\cdots;\Psi_{0n},\cdots,\Psi_{hn})$$

where

$$\Psi_{hi}=w_h^{(i)}(T''_{01},\cdots,T''_{0m};\cdots;T''_{h1},\cdots,T''_{hm})$$

and

$$T''_{hi}=\phi_h(T_{0i},T'_{0i},T_{1i},T'_{1i},\cdots,T_{hi},T'_{hi})$$

($\phi=(\phi_h)$ now stands, as in no. 8, for the group law of the hyperexponential group H). We thus obtain a polynomial in the T''_{hi}, which (by the argument of no. 7) can be expressed as a linear combination of the polynomials

$$E_\lambda(T''_{01},\cdots,T''_{0m};\cdots;T''_{h1},\cdots,T''_{hm};\cdots). \tag{35}$$

Let us now go over to the quotient algebras $P/\mathfrak{a}$ and $Q/\mathfrak{b}$; let X'_{hi}, Y'_{hi} correspond to S'_{hi}, T'_{hi} by the natural mapping, and, changing slightly the notations of no. 8, let us write

$$Z_\alpha{}^0=\sum_{0\leq\beta\leq\alpha} E_\beta(X_{01},\cdots,X_{hn},\cdots)E_{\alpha-\beta}(X'_{01},\cdots,X'_{hn},\cdots)$$

$$\bar{Z}_\lambda{}^0=\sum_{0\leq\mu\leq\lambda} E_\mu(Y_{01},\cdots,Y_{hm},\cdots)E_{\lambda-\mu}(Y'_{01},\cdots,Y'_{hm},\cdots).$$

Then the image, by $\boldsymbol{s}'\otimes\boldsymbol{s}'$, of $Z_\alpha{}^0$, is obtained as a linear combination of the elements (35) in which T_{hi} and T'_{hi} have been respectively replaced by Y_{hi} and Y'_{hi}; but these elements are merely the elements $\bar{Z}_\lambda{}^0$, by the argument of no. 8. The conditions of [5, Prop. 2] are thus satisfied, and the proof of Theorem 4 is brought to an end.

17. We will say that the homomorphism $\boldsymbol{s}$ of G into $\bar{G}$, defined above, is *associated* to the matrix $\boldsymbol{W}$. We now prove (with the same notations):

THEOREM 5. *Suppose K is a perfect field. Every homomorphism $\boldsymbol{s}$ of G into $\bar{G}$ is associated to an $n\times m$ matrix $\boldsymbol{W}$ with elements in $\mathcal{E}^+(K)$.*

We are going to construct a matrix $\boldsymbol{W}$ for which relations (31) will hold. We can write first

$$\boldsymbol{s}'(X_{0i}) = \sum_{j=1}^{m} a_{ij} Y_{0j} \qquad (1 \leq i \leq n).$$

We consider the Witt-vectors $A_{ij} = (a_{ij}, 0, 0, \cdots)$, and the matrix $\boldsymbol{W}^{(0)} = (A_{ij})$; we have therefore

$$\boldsymbol{s}'(X_{0i}) = w_0^{(0,i)}(Y_{01}, \cdots, Y_{0m}) \qquad (1 \leq i \leq n).$$

As a basis for an inductive argument, suppose we have constructed a matrix $\boldsymbol{W}^{(r)}$ such that

$$\boldsymbol{s}'(X_{hi}) = w_h^{(r,i)}(Y_{01}, \cdots, Y_{0m}; \cdots; Y_{h1}, \cdots, Y_{hm}) \tag{36}$$

for $1 \leq i \leq n$ and $0 \leq h \leq r$. As $\boldsymbol{s}'$ is a homomorphism of hyperalgebras, we have, by (18)

$$\boldsymbol{s}'(Z_\alpha) = E_\alpha(\boldsymbol{s}'(X_{01}), \cdots, \boldsymbol{s}'(X_{hn}), \cdots). \tag{37}$$

We prove that the differences

$$U_i = \boldsymbol{s}'(X_{r+1,i}) - w_{r+1}^{(r,i)}(Y_{01}, \cdots, Y_{0m}; \cdots; Y_{r+1,1}, \cdots, Y_{r+1,m})$$

are *derivations* in $\bar{G}$ $(1 \leq i \leq n)$. We have by definition

$$\begin{aligned}(\boldsymbol{s}' \otimes \boldsymbol{s}')(X_{r+1,i}{}^0) &= I \otimes \boldsymbol{s}'(X_{r+1,i}) + \boldsymbol{s}'(X_{r+1,i}) \otimes I \\ &\quad + \sum_{0<k<p^{r+1}} \boldsymbol{s}'(Z_{k\epsilon_i}) \otimes \boldsymbol{s}'(Z_{(p^{r+1}-k)\epsilon_i}).\end{aligned} \tag{38}$$

Now in the sum in the right hand side of this formula, we can replace $\boldsymbol{s}'(Z_{k\epsilon_i})$ by its expression (37), and as $k < p^{r+1}$, only terms $\boldsymbol{s}'(X_{hi})$ with $h \leq r$ will intervene. These can then be replaced by their expression (36). Now, using (22) with $\alpha = p^{r+1}\epsilon_i$ (and therefore $E_\alpha(\boldsymbol{x}) = \boldsymbol{x}_{r+1}{}^{(i)}$), we see that we have

$$\begin{aligned}&w_{r+1}{}^{(r,i)}(Y_{01}{}^0, \cdots, Y_{0m}{}^0; \cdots; Y_{r+1,1}{}^0, \cdots, Y_{r+1,m}{}^0) \\ &= I \otimes w_{r+1}{}^{(r,i)}(Y_{01}, \cdots, Y_{r+1,m}) + w_{r+1}{}^{(r,i)}(Y_{01}, \cdots, Y_{r+1,m}) \otimes I \\ &\quad + \sum_{0<k<p^{r+1}} \boldsymbol{s}'(Z_{k\epsilon_i}) \otimes \boldsymbol{s}'(Z_{(p^{r+1}-k)\epsilon_i})\end{aligned} \tag{39}$$

since $\boldsymbol{W}^{(r)}$ defines a homomorphism $\boldsymbol{w}^{(r)}$ of H^m into H^n. As computations with tensor products and with "Leibniz formulae" are "dual" to each other (see for instance [4, proof of Lemma 2]), comparison of (38) and (39) shows that $U_i(fg) = f \cdot U_i g + g \cdot U_i f$.

We can therefore write

$$U_i = \sum_{j=1}^{m} a_{ij}{}^{(r+1)} Y_{0j} \qquad (1 \leq i \leq n).$$

Consider the Witt vectors $A_{ij}^{(r+1)} = (a^{(r+1)}, 0, 0, \cdots)$, and the matrix $\boldsymbol{W}^{(r+1)} = \boldsymbol{W}^{(r)} + \boldsymbol{t}^{r+1} \cdot (A_{ij}^{(r+1)})$. It is then clear that we have the relations

$$\boldsymbol{s}'(X_{hi}) = w_h^{(r+1,i)}(Y_{01}, \cdots, Y_{0m}; \cdots; Y_{h1}, \cdots, Y_{hm})$$

for $1 \leq i \leq n$ and $0 \leq h \leq r+1$. The induction is then concluded in the usual way, the matrices $\boldsymbol{W}^{(r)}$ "converging" obviously towards a matrix $\boldsymbol{W}$ for which relations (31) are verified for every h. Theorem 5 is therefore proved.

18. The result embodied in Theorems 4 and 5 can be put in a much more suggestive form. Multiplying on the left both sides of (32) by $\boldsymbol{t}$ gives an equivalent condition, since the ring $\mathcal{E}^+(K)$ has no zero-divisors; using the commutation rules (7), we see therefore that (32) is equivalent to the relation

$$(\boldsymbol{\pi I}_n - \boldsymbol{tU})\boldsymbol{W} = (\boldsymbol{W} + \boldsymbol{tL})(\boldsymbol{\pi I}_m - \boldsymbol{tV}) \tag{40}$$

($\boldsymbol{I}_m$ and $\boldsymbol{I}_n$ being the unit matrices of order m and n). Conversely, suppose there is an $n \times m$ matrix $\boldsymbol{W}_1$ such that

$$(\boldsymbol{\pi I}_n - \boldsymbol{tU})\boldsymbol{W} = \boldsymbol{W}_1(\boldsymbol{\pi I}_m - \boldsymbol{tV}). \tag{41}$$

From such a relation, it follows at once that $\boldsymbol{W}$ and $\boldsymbol{W}_1$ are congruent mod. $\boldsymbol{t}$, in other words we can write $\boldsymbol{W}_1 = \boldsymbol{W} + \boldsymbol{tL}$, and we see therefore that (41) implies (40), hence also (32). The existence of an $n \times m$ matrix $\boldsymbol{W}_1$ over $\mathcal{E}^+(K)$ satisfying (41) is therefore (when K is perfect) the necessary and sufficient condition for $\boldsymbol{W}$ to represent a homomorphism of G into $\bar{G}$. But this can also be formulated in different terms: consider the left-modules $E = (\mathcal{E}^+(K))^n$, $F = (\mathcal{E}^+(K))^m$, direct sums of n (resp. m) modules identical to $\mathcal{E}^+(K)$ (considered as a left module over itself). In E (resp. F), let M (resp. N) be the submodule which is the image of E (resp. F) under the endomorphism represented by the matrix $\boldsymbol{\pi I}_n - \boldsymbol{tU}$ (resp. $\boldsymbol{\pi I}_m - \boldsymbol{tV}$). Relation (41) is then the necessary and sufficient condition for the matrix $\boldsymbol{W}$ to represent an $(\mathcal{E}^+(K))$-homomorphism of the module E into the module F, which sends M into N, and therefore to define *a homomorphism of E/M into F/N*. We thus see that, by associating with the group G the $\mathcal{E}^+(K)$-module E/M, *the theory of abelian formal Lie groups over a perfect field K is essentially reduced to the theory of left $\mathcal{E}^+(K)$-modules.*

19. Applications: I. Classification of abelian Lie groups. If $\boldsymbol{s}$ is an isomorphism of G onto $\bar{G}$ (for $m = n$), the matrix (a_{ij}) (with the notations of no. 17) must be invertible, and from that remark it is very easy to conclude that both matrices $\boldsymbol{W}$ and $\boldsymbol{W}_1$ in (41) must be invertible. Therefore:

THEOREM 6. *Let K be a perfect field. In order that two abelian Lie groups G, $\bar{G}$ over K, respectively associated to two square matrices $\boldsymbol{U}$, $\boldsymbol{V}$ of order n, with elements in $\mathcal{E}^+(K)$, be isomorphic, it is necessary and sufficient that $\pi\boldsymbol{I} - t\boldsymbol{U}$ and $\pi\boldsymbol{I} - t\boldsymbol{V}$ be equivalent.*

In the language of modules, this (with the notations of no. 18) means that the modules E/M and E/N associated to G and $\bar{G}$ are *isomorphic*. The classification of abelian Lie groups over a perfect field K is therefore equivalent to the classification of the $\mathcal{E}^+(K)$-modules having a finite system of generators to which they correspond; as mentioned in the Introduction, no satisfactory theory is known at present for such modules, due to the fact that $\mathcal{E}^+(K)$ is not a principal ideal ring.

It follows of course from (32) that G and $\bar{G}$ will be isomorphic if there exists an invertible matrix $\boldsymbol{W}$ such that $\boldsymbol{W}^{\sigma}\boldsymbol{U}\boldsymbol{W}^{-1} = \boldsymbol{V}$, but this condition is by no means necessary, as we shall see below, and the problem of classifying matrices under this stronger equivalence relation does not appear to be much easier, even when K is algebraically closed. When $\boldsymbol{U}$ is invertible and K algebraically closed, there is always an invertible matrix $\boldsymbol{W}$ such that $\boldsymbol{W}^{\sigma}\boldsymbol{U}\boldsymbol{W}^{-1} = \boldsymbol{I}$, as was essentially proved in [4, no. 13]; the corresponding groups are therefore all isomorphic to $(W_1{}^*)^n$. A similar proof would show that, when K is algebraically closed and $\boldsymbol{U} = t^r\boldsymbol{U}_1$, with $\boldsymbol{U}_1$ invertible, there exists $\boldsymbol{W}$ such that $\boldsymbol{W}^{\sigma}\boldsymbol{U}\boldsymbol{W}^{-1} = t^r\boldsymbol{I}$, and the corresponding groups are therefore isomorphic to the direct product $(I_r)^n$.

In particular, for the groups of "symmetric braid" type [5, no. 10], we have

$$\boldsymbol{U} = \begin{pmatrix} 0 & t^r \\ t^r & 0 \end{pmatrix} = t^r \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}$$

and therefore (as announced in [5]) if K is algebraically closed, these groups are isomorphic to products $I_r \times I_r$. Similarly, the groups of the "tree" type, corresponding to matrices

$$\begin{pmatrix} 0 & t^r \\ 0 & t^s \end{pmatrix}$$

do not yield new types of groups for $r \geq s$, for the matrix is then

$$\boldsymbol{U} = t^s \begin{pmatrix} 0 & t^{r-s} \\ 0 & I \end{pmatrix}$$

and it is readily verified that the matrix $\boldsymbol{W} = \begin{pmatrix} I & -t^{r-s} \\ 0 & I \end{pmatrix}$ is such that $\boldsymbol{W}^{\sigma}\boldsymbol{U}\boldsymbol{W}^{-1} = \begin{pmatrix} 0 & 0 \\ 0 & t^s \end{pmatrix}$, so that the group is isomorphic to $W_1 \times I_s$ (as was conjectured in [5, no. 10]).

Going now to the other extreme, let us consider the case in which K is the prime field $\boldsymbol{F}_p$, and let us investigate the classification of *one-dimensional* abelian groups over K. As σ is then the identity, $\mathcal{E}^+(K)$ is a commutative ring, and the problems amounts, according to Theorem 6, to classify elements of that ring under the equivalence relation

$$\boldsymbol{\pi} - \boldsymbol{ta} = \boldsymbol{c}(\boldsymbol{\pi} - \boldsymbol{tb}) \tag{42}$$

where $\boldsymbol{c}$ is invertible. We have of course

$$\boldsymbol{a} = A_0 + \boldsymbol{t}A_1 + \cdots + \boldsymbol{t}^k A_k + \cdots$$

where the $A_k = (a_{k0}, a_{k1}, \cdots)$ are Witt-vectors with components in $\boldsymbol{F}_p$, and similarly for $\boldsymbol{b}$ and $\boldsymbol{c}$. It is then easily verified that, given $\boldsymbol{b}$, it is possible to determine $\boldsymbol{c}$ in one and only one way, such that all the elements $a_{ki} = 0$ for $i > 0$. The "first" elements a_{k0} are then invariants of the class of abelian groups; as they can be chosen arbitrarily in $\boldsymbol{F}_p$, we see that the set of classes of non isomorphic abelian groups (isomorphism being meant in the sense of $\boldsymbol{F}_p$-isomorphism) has the *power of the continuum* (in sharp distinction to the corresponding situation in the case of an algebraically closed field K). We may also observe that in this case, the relation $\boldsymbol{W}^{\sigma}\boldsymbol{U}\boldsymbol{W}^{-1} = \boldsymbol{V}$ would reduce to $\boldsymbol{a} = \boldsymbol{b}$ instead of (42).

20. Applications: II. Analytically simple abelian Lie groups. We now want to show that there exist abelian Lie groups of dimension > 1 which have *no nontrivial subgroup*, and can therefore be called "analytically simple" groups. More precisely, we will exhibit a group G of dimension 2 such that there exists *no non zero homomorphism of a group of dimension* 1 *into* G. G will be a group of the "dissymetric braid" type, corresponding to the matrix $\begin{pmatrix} 0 & \boldsymbol{t}^2 \\ \boldsymbol{t} & 0 \end{pmatrix}$. We may suppose that K is algebraically closed, and then a one-dimensional group will correspond to a one-element matrix of type $\boldsymbol{t}^q$. The existence of a homomorphism of this last group into G means that there exist elements $\boldsymbol{a}$, $\boldsymbol{a}'$, $\boldsymbol{b}$, $\boldsymbol{b}'$ in $\mathcal{E}^+(K)$, such that

$$(\boldsymbol{\pi} - \boldsymbol{t}^{q+1})(\boldsymbol{a}\ \boldsymbol{a}') = (\boldsymbol{b}\ \boldsymbol{b}')\begin{pmatrix} \boldsymbol{\pi} & -\boldsymbol{t}^2 \\ -\boldsymbol{t}^2 & \boldsymbol{\pi} \end{pmatrix} \tag{43}$$

which is equivalent to

$$\begin{cases} (\boldsymbol{\pi} - \boldsymbol{t}^{q+1})\boldsymbol{a} = \boldsymbol{b}\boldsymbol{\pi} - \boldsymbol{b}'\boldsymbol{t}^2 \\ (\boldsymbol{\pi} - \boldsymbol{t}^{q+1})\boldsymbol{a}' = \boldsymbol{b}'\boldsymbol{\pi} - \boldsymbol{b}\boldsymbol{t}^2. \end{cases} \tag{44}$$

We write $\boldsymbol{a} = \sum_k \boldsymbol{t}^k A_k$, $\boldsymbol{a}' = \sum_k \boldsymbol{t}^k A'_k$, $\boldsymbol{b} = \sum_k \boldsymbol{t}^k B_k$, $\boldsymbol{b}' = \sum_k \boldsymbol{t}^k B'_k$, where the

A_k, A'_k, B_k, B'_k are Witt vectors. It follows from the proof of Theorem 5 (or by a direct argument from (41)) that we can suppose $A_k = (a_{k0}, 0, 0, \cdots)$, $A'_k = (a'_{k0}, 0, 0, \cdots)$; on the other hand, we can suppose that $\boldsymbol{b}$ and $\boldsymbol{b'}$ are not both divisible by a power of $\boldsymbol{t}$, since otherwise $\boldsymbol{a}$ and $\boldsymbol{a'}$ would also be divisible by it, and we would then be reduced to the first case. We remark finally that we have $q > 0$, since there are no homomorphisms of the multiplicative group into G which are not trivial, the hyperalgebra of G being a nilalgebra.

1. Suppose $B_0 = (b_{00}, b_{01}, \cdots) \neq 0$. Identifying the coefficients of $\boldsymbol{t}^0$ in the first equation (44) gives $A_0 = B_0$, hence $a_{00} = b_{00} \neq 0$ and $b_{0i} = 0$ for $i > 0$. We cannot have $q = 1$, for in that case, identifying the coefficients of $\boldsymbol{t}^2$ in the second equation (44) would give $\boldsymbol{\pi} A'_2 - A'_0 = \boldsymbol{\pi} B'_2$, hence $a'_{00} = 0$, and $A'_0 = 0$; but then, the same equation would give $B'_0 = A'_0 = 0$, and identifying the coefficients of $\boldsymbol{t}^2$ in the first equation (44) would give $\boldsymbol{\pi} A_2 - A_0 = \boldsymbol{\pi} B_2$, which contradicts $a_{00} \neq 0$. The identification of the coefficients of $\boldsymbol{t}^2$ in the first equation gives then (since $q > 1$), $\boldsymbol{\pi} A_2 = \boldsymbol{\pi} B_2 - B'_0{}^{\sigma^2}$, and if $B'_0 = (b'_{00}, b'_{01}, \cdots)$, this yields $b'_{00} = 0$. As $A'_0 = B'_0$, we have also $a'_{00} = 0$. Now, if $q = 2$, we obtain by identifying the terms in $\boldsymbol{t}^3$ in the second equation (44),

$$\boldsymbol{\pi} A'_3 - A'_0 = \boldsymbol{\pi} B'_3 - B_0{}^{\sigma^3}$$

and this yields $b_{00} = 0$, contrary to assumption; if on the other hand $q > 2$, we obtain similarly $\boldsymbol{\pi} A'_3 = \boldsymbol{\pi} B'_3 - B_0{}^{\sigma^3}$, and we reach again a contradiction.

2. Suppose now $B'_0 \neq 0$; then we have in the same way $A'_0 = B'_0$, hence $a'_{00} = b'_{00} \neq 0$ and $b'_{0i} = 0$ for $i > 0$. We see as in 1. that we cannot have $q = 1$; but if $q > 1$, the relation $\boldsymbol{\pi} A_2 = \boldsymbol{\pi} B_2 - B'^{\sigma^2}$ gives $b'_{00} = 0$, hence again a contradiction. It is therefore impossible to satisfy (43) when $\boldsymbol{a}$ and $\boldsymbol{a'}$ are not both 0.

A similar argument shows that if G is associated to the matrix $\begin{pmatrix} 0 & \boldsymbol{t}^s \\ \boldsymbol{t}^r & 0 \end{pmatrix}$ with $r < s$, then G is analytically simple if $s + r$ is *odd*; but if $s + r = 2h$, there is a nontrivial homomorphism of the one-dimensional group corresponding to $\boldsymbol{t}^h$ into G. These examples seem to show that the determination of all abelian analytically simple groups is a problem of great complexity.

21. Applications: III. Duality of abelian Lie groups. Suppose that K is the *prime field* $\boldsymbol{F}_p$; then the ring $\mathcal{E}^+(K)$ is commutative and the transposed matrix of any matrix with elements in that ring is again a matrix

with elements in $\mathcal{E}^+(K)$ (whereas in general it is a matrix over the opposite ring). If, to each square matrix $\boldsymbol{U}$ with elements in $\mathcal{E}^+(K)$, we associate its transposed matrix ${}^t\boldsymbol{U}$, we are defining a pairing between the associated groups, which we can call *dual* to each other. If the matrix $\boldsymbol{W}$ represents a homomorphism of G into $\bar{G}$, then it follows from (41) that ${}^t\boldsymbol{W}_1$ represents a homomorphism of the dual $\bar{G}^*$ of $\bar{G}$ into the dual G^* of G; we will say that this homomorphism is *transposed* of the homomorphism represented by $\boldsymbol{W}$; the usual rules concerning transposed homomorphisms are then valid.

One-dimensional groups (over $\boldsymbol{F}_p$) are obviously isomorphic to their dual; so are two-dimensional groups of the "streak" or "braid" type; it is an open question whether an abelian Lie group is always isomorphic to its dual.

NORTHWESTERN UNIVERSITY.

BIBLIOGRAPHY.

[1] J. Dieudonné, "Groupes de Lie et hyperalgèbres de Lie sur un corps de caractéristique $p > 0$," *Commentarii Mathematici Helvetici*, vol. 28 (1954), pp. 87-118.

[2] ———, "Sur la notion de variables canoniques," *Anais da Academia Brasileira de Ciencias*, vol. 27 (1955).

[3] ———, "Le calcul différentiel dans les corps de caractéristique $p > 0$." *Proceedings of the International Congress of Mathematicians*, 1954, vol. 2.

[4] ———, "Lie groups and Lie hyperalgebras over a field of characteristic $p > 0$, (II)," *American Journal of Mathematics*, vol. 77 (1955), pp. 218-244.

[5] ———, "Groupes de Lie et hyperalgèbres de Lie sur un corps de caractéristique $p > 0$ (III)," *Mathematische Zeitschrift*, vol. 62 (1955).

[6] ———, "Witt groups and hyperexponential groups," *Mathematika*, vol. 2 (1955).

[7] E. Witt, "Zyklische Körper und Algebren der Charakteristik p vom Grad p^n," *Journal für die Reine und Angewandte Mathematik*, vol. 176 (1937), pp. 126-140.

ON THE LOCAL BEHAVIOR OF SOLUTIONS OF NON-PARABOLIC PARTIAL DIFFERENTIAL EQUATIONS.

III. Approximations by spherical harmonics.*

By PHILIP HARTMAN and AUREL WINTNER.

In this paper, the analogues of the theorems of [4], [5] on solutions of elliptic partial differential equations will be obtained for the case where the number of independent variables exceeds 2. For the sake of notational simplicity, it will be assumed that the number of independent variables is 3. The equation to be considered is of the type $\Delta u + \cdots = 0$, where Δu is the Euclidean Laplacian of u, and no second order partial derivative of u occurs in the rest of the equation. The replacement of Δu by a more general linear combination of second derivatives of u will not be considered at this time. (In the plane, this more general case can be reduced to the special case by conformal mappings under suitable smoothness assumptions on the coefficients; in space, perturbation methods of Korn and Lichtenstein can be used.) For simplicity, the partial differential equation to be considered will be assumed to be linear (the methods are applicable to non-linear equations of the type (5)-(6) below).

The first part of the paper deals with solutions near a zero, the second part with solutions near an isolated singularity.

Part 1. The zeros of a solution.

1. Statement of the theorems. In the linear elliptic partial differential equation

$$\Delta u + a \cdot \nabla u + \gamma u = 0, \tag{1}$$

let Δu denote the (Euclidean) Laplacian, ∇u the gradient of u, $a = a(x)$ a vector and $\gamma = \gamma(x)$ a scalar function of the position vector x, finally $a \cdot \nabla u$ the scalar product of a and ∇u. It is known ([4], pp. 449-450) that if the number of independent variables in (1) is 2, say $x = (x_1, x_2)$, if $a(x)$ and $\gamma(x)$ are continuous in a vicinity of $x = 0$ and if $u = u(x)$ is a C^2-solution (or even a C^1-solution in an appropriate sense) vanishing at

* Received April 18, 1955.

$x=0$, then either $u(x)\equiv 0$ or there exist an integer $N>0$ and constants $(c_1, c_2)\neq(0,0)$ such that, as $r=|x|\to 0$,

$$u(x)=c_1 r^N\cos N\phi+c_2 r^N\sin N\phi+o(r^N),$$
$$\nabla u(x)=\nabla(c_1 r^N\cos N\phi+c_2 r^N\sin N\phi)+o(r^{N-1}). \tag{2}$$

uniformly in ϕ, where $x=(x_1,x_2)=(r\cos\phi, r\sin\phi)$. The proof of this fact depended on an adaptation of a proof of a uniqueness theorem of Carleman [2].

The object of this chapter is to obtain similar asymptotic formulae in case the number of independent variables in (1) exceeds 2. The methods used to prove (2), depending on function theory, cannot be applied in this situation. They will be replaced by procedures depending on Fourier analysis and on a generalization of the argument used by C. Müller [6] to obtain an extension of Carleman's uniqueness theorem in the plane to a uniqueness theorem in space.

The analogue of (2) will be

$$u(x)=r^N S_N(e)+o(r^N),$$
$$\nabla u(x)=\nabla(r^N S_N(e))+o(r^{N-1}), \tag{3}$$

where $S_N(e)$ is a spherical harmonic of order N. Here and in the sequel, $x=re$, where $r=|x|$; so that e is a unit vector.

THEOREM 1. *Let x be a 3-dimensional vector, $a=a(x)$ a 3-dimensional continuous vector and $\gamma=\gamma(x)$ a continuous scalar function in a sphere about $x=0$, say $0\leqq|x|\leqq 1$. Let $u=u(x)$ be a C^1-solution of (1) on $|x|\leqq 1$ satisfying*

$$u(0)=0. \tag{4}$$

Then either $u(x)\equiv 0$ on $|x|\leqq 1$ or there exist an integer $N>0$ and a spherical harmonic $S_N(e)\not\equiv 0$ of order N on the unit sphere $|x|=1$ with the property that the relations (3) hold uniformly in e, as $r=|x|\to 0$.

A function $u=u(x)$ is called a C^1-solution of (1) on $|x|\leqq 1$ if it is of class C^1 and can be represented as the sum of an harmonic function and the Newtonian potential of $(a\cdot\nabla u+\gamma u)/4\pi$.

Remark 1. It will be clear from the proof that Theorem 1 remains correct if the dimension number 3 is replaced by any dimension number.

Remark 2. It will also be clear that Theorem 1 remains true if (1) is replaced by a non-linear equation

$$\Delta u + g(x, u, \nabla u) = 0, \tag{5}$$

where $g(x, u, \nabla u)$ is a continuous function of its (seven) variables on a set $|x| \leqq 1$, $|u| \leqq$ const., $|\nabla u| \leqq$ const. and is subject to an inequality of the form

$$|g(x, u, \nabla u)| \leqq \text{Const.}\,(|u| + |\nabla u|). \tag{6}$$

Remark 3. The $o(r^N)$- and $o(r^{N-1})$-terms in (3) can be replaced by $O(r^{N+1}|\log r|)$ and $O(r^N|\log r|)$, respectively. This improvement of (3) follows by repeating the arguments of Sections 6 and 7 below with (61) replaced by the estimates, $u = O(r^N)$ and $\nabla u = O(r^{N-1})$, supplied by (3). A similar remark applies to Theorems 1 bis and 4 below and to the corresponding theorems of [4], [5].

As a consequence of Theorem 1, there results the following corollary which is an analogue (and extension) of Carleman's theorem [2] for two independent variables:

COROLLARY 1. *Let $a(x)$, $\gamma(x)$ and $u(x)$ satisfy the condition of Theorem 1 and, in addition, let*

$$u(x) = o(r^n) \text{ for } n = 0, 1, \cdots \tag{7}$$

as $r \to 0$. Then $u(x) \equiv 0$ on $|x| \leqq 1$.

Another consequence of Theorem 1 is the following:

COROLLARY 2. *Let $a(x)$, $\gamma(x)$, $u(x)$ satisfy the assumptions of Theorem 1. Then the zeros of $\nabla u(x)$ cannot cluster at $x = 0$ unless $u(x) \equiv 0$ on $|x| \leqq 1$.*

In another direction, Theorem 1 can be extended as follows:

THEOREM 1 bis. *Let $a = a(x)$ and $\gamma = \gamma(x)$ be, respectively, a vector and scalar function of class C^1 in a vicinity of $x = 0$. Let $u = u(x) \not\equiv 0$ be a C^2-solution of (1) in a vicinity of $x = 0$ satisfying (4) (so that there exist an integer $N > 0$ and a spherical harmonic $S_N(e) \not\equiv 0$ satisfying (3)). Then the Hessian matrix of u, say u_{xx}, satisfies, as $r \to 0$,*

$$u_{xx} = (r^N S_N(e))_{xx} + o(r^{N-2}). \tag{3 bis}$$

The details of the proof of this theorem will be omitted. It can be obtained by considering the inhomogeneous system of equations,

$$\Delta u_k + a \cdot \nabla u_k + \gamma u_k + a_k \cdot \nabla u + \gamma_k u = 0, \qquad (k = 1, 2, 3),$$

for the components of the gradient $\nabla u = (u_1, u_2, u_3)$, obtained by differentiating (1), and modifying the proof of Theorem 1 in a manner analogous to that used in [4], pp. 467-469.

2. An estimate for $\| u - u^N \|$. In what follows, x will denote a 3-dimensional vector. When it is necessary to deal with components of x, these will be denoted by (x, y, z); there will be no confusion over this double use of x. The geographical coordinates of a point e on the unit sphere

$$B: \ |e| = 1 \tag{8}$$

will be denoted by (θ, ϕ). Hence $x = (r\cos\phi\sin\theta, r\sin\phi\sin\theta, r\cos\theta)$, where $r = |x|$. A function $u = u(x)$ can be considered as a function of r and e, say $u = u(r, e)$. The symbol $\| \cdots \|$ will refer to the L^2-norm on (8); thus $\| u(r, e) \|$ becomes a function of r. The element of area on (8) will be denoted by $d\sigma$.

Let $S_{nj}(e)$ be the spherical harmonic

$$S_{nj} = c_{nj}P_{nj}(\theta)\cos j\phi \text{ or } S_{n\,j+n} = c_{nj}P_{nj}(\theta)\sin j\phi \tag{9}$$

for $j = 0, 1, \cdots, n$ or $j = 1, \cdots, n$, respectively, and $n = 0, 1, \cdots$, where the $P_{nj}(\theta)$ are the Legendre functions and the c_{nj} are normalizing factors. Thus S_{nj}, where $j = 0, \cdots, 2n$ and $n = 0, 1, \cdots$, is a complete orthonormal sequence on (8).

Let a function $u = u(x)$ of $x = re$, where $r = |x|$, be written as a function $u(r, e)$. If, for a fixed $r > 0$, the functions $f(x) = f(r, e)$ and $u(x) = u(r, e)$ are of class L^2 on (8), let

$$F_{nj}(r) = \int_B\int f(r, e)S_{nj}(e)d\sigma, \tag{10}$$

$$U_{nj}(r) = \int_B\int u(r, e)S_{nj}(e)d\sigma \tag{11}$$

denote the respective Fourier constants. Thus, $u(r, e)$ has the Fourier series

$$u(r, e) \sim \sum_{n=0}^{\infty}\sum_{j=0}^{2n} U_{nj}(r)S_{nj}(e); \tag{12}$$

$u^N(r, e)$ will denote the partial sum

$$u^N(r, e) = \sum_{n=0}^{N}\sum_{j=0}^{2n} U_{nj}(r)S_{nj}(e). \tag{13}$$

Let $f(x)$ be a continuous function on $|x| \leqq 1$ and let $u = u(x)$ be a C^1-solution of the Poisson equation

$$\Delta u = f. \tag{14}$$

The main equalities will furnish estimates, as $r \to 0$, for $U_{nj}(r)$ and $\| u(r,e) - u^N(r,e) \|^2$ in terms of

$$\Phi(r) = \| f(r,e) \|^2. \tag{15}$$

LEMMA 1. *Let $f(x)$ be a continuous function on $|x| \leqq 1$ and let $u(x)$ be a C^1-solution of* (14). *Let λ be a (non-negative) number and N an integer satisfying*

$$N > \lambda + \tfrac{1}{2}. \tag{16}$$

Then there exists a constant C (independent of N and λ) with the property that, for $0 < r \leqq 1$,

$$\| u - u^N \|^2 \leqq C\chi(r), \tag{17}$$

where

$$\chi(r) = r^{2N+2} + r^{2\lambda+3}(2N - 2\lambda - 1)^{-1} \int_0^1 s^{-2\lambda}\Phi(s)\,ds \quad (\leqq \infty). \tag{18}$$

The constant C depends only on bounds for $|u|$, $|\nabla u|$ on $|x| = 1$.

3. Proof of Lemma 1. If $u = u(x)$ is of class C^2, then differentiations under the integral sign show that, by virtue of (14) and (10), the function (11) satisfies the singular inhomogeneous differential equation

$$(r^2U')' - n(n+1)U = r^2F, \qquad \text{where } ' = d/dr, \tag{19}$$

$U = U_{nj}$ and $F = F_{nj}$. The general solution $U = U(r)$ of (19), continuous at $r = 0$, is

$$U(r) = (2n+1)^{-1}\{r^n(A - \int_r^1 s^{1-n}F(s)ds) - r^{-1-n}\int_0^r s^{n+2}F(s)ds\}, \tag{20}$$

where $A = A_{nj}$ is a constant. Since u is of class C^1, it follows that the derivative

$$U_{nj}'(r) = \int\!\!\int_B u_r(r,e)S_{nj}(e)\,d\sigma \tag{21}$$

exists, is continuous and can be obtained by a differentiation of (20):

$$U'(r) = (2n+1)^{-1}\{nr^{n-1}(A - \int_r^1 s^{1-n}F(s)ds) + (n+1)r^{-2-n}\int_0^r s^{n+2}F(s)ds\}. \tag{22}$$

The formulae (20) and (22), just derived under the assumption that

$u = u(x)$ is of class C^2, are valid if $u = u(x)$ is only of class C^1. This follows, for example, by approximating f and u by smooth functions.

By letting $r = 1$ in (20) and (22),

$$A = (n+1)U(1) + U'(1) \qquad (A = A_{nj}, U = U_{nj}). \tag{23}$$

Hence, by Bessel's inequality,

$$\sum_{n=0}^{\infty} \sum_{j=0}^{2n} A^2/(n+1)^2 \leqq \text{const.}\ (\| u \|^2 + \| u_r \|^2)_{r=1} < \infty. \tag{24}$$

The relation (20) shows that

$$\tfrac{1}{3}(2n+1)^2 U^2 \leqq A^2 r^{2n} + r^{2n}\Big(\int_r^1 s^{1-n}F(s)ds\Big)^2 + r^{-2-2n}\Big(\int_0^r s^{n+2}F(s)ds\Big)^2. \tag{25}$$

In view of Schwarz's inequality,

$$\Big(\int_r^1 s^{1-n}F(s)ds\Big)^2 \leqq \Big(\int_r^\infty s^{2(1-n+\lambda)}ds\Big)\Big(\int_r^1 s^{-2\lambda}F^2(s)ds\Big),$$

if $2(n-\lambda-1) > 1$, that is, if $n > \lambda + \frac{3}{2}$. Similarly,

$$\Big(\int_0^r s^{n+2}F(s)ds\Big)^2 \leqq \Big(\int_0^r s^{2(n+\lambda+2)}ds\Big)\Big(\int_0^r s^{-2\lambda}F^2(s)ds\Big).$$

The last three formula lines give

$$\tfrac{1}{3}(2n+1)^2 U^2 \leqq A^2 r^{2n} + r^{2\lambda+3}(2n-2\lambda-3)^{-1}\int_r^1 s^{-2\lambda}F^2(s)ds + r^{2\lambda+3}(2n+2\lambda+5)^{-1}\int_0^r s^{-2\lambda}F^2(s)ds, \tag{26}$$

if $n > \lambda + \frac{3}{2}$. If this relation is divided by $(2n+1)^2$ and the resulting inequality summed over $n = N+1, N+2, \cdots$ and $j = 0, \cdots, 2n$, where $N > \lambda + \frac{1}{2}$, then Parseval's relation shows that

$$\| u - u^N \|^2 \leqq 3 \sum_{n=N+1}^{\infty} \sum_{j=0}^{2n} r^{2n} A_{nj}{}^2/(2n+1)^2 + 3r^{2\lambda+3}(2N-2\lambda-1)^{-1}\int_0^1 s^{-2\lambda}\Phi(s)ds. \tag{27}$$

In view of (24), this leads to (17)-(18).

4. The derivatives u_r, u_ϕ. Note that, in the deduction of (27) from (26), the factor $(2n+1)^{-2}$ in the expressions leading to the last term in (27) was replaced by 1. Since (22) and (25) show that

$$\tfrac{1}{3}(2n+1)^2 r^2 U'^2 \leqq (n+1)^2\{\cdots\}, \tag{28}$$

where $\{\cdots\}$ is the expression on the right side of the inequality (25), the proof of Lemma 1 implies

LEMMA 2. *Let u, f, N, λ satisfy the conditions of Lemma* 1. *Then there exist a constant C (independent of N and λ) with the properties that, for $0 < r < 1$,*

$$r^2 \| u_r - u_r^N \|^2 \leqq C\chi^*(r), \tag{29}$$

where

$$\chi^*(r) = N^2 r^{2N+2}(1-r^2)^{-3} + r^{2\lambda+3}(2N-2\lambda-1)^{-1}\int_0^1 s^{-2\lambda}\Phi(s)ds. \tag{30}$$

In fact, the analogue of (27) is

$$r^2 \| u_r - u_r^N \|^2 \leqq 3\sum_{n=N+1}^{\infty}\sum_{j=0}^{2n} r^{2n}A_{nj}^2 + 3r^{2\lambda+3}(2N-2\lambda-1)^{-1}\int_0^1 s^{-2\lambda}\Phi(s)ds,$$

since $(n+1)^2/(2n+1)^2 \leqq 1$. In view of (24),

$$\sum_{j=0}^{2n} A_{nj}^2 = o(n^2) \quad \text{as} \quad n \to \infty.$$

Clearly, (29)-(30) follows from the last two formula lines.

A statement analogous to Lemma 2 will be obtained for the case where ru_r is replaced by the partial derivative u_ϕ.

LEMMA 3. *Let u, f, N, λ satisfy the conditions of Lemma* 1. *Then there exists a constant C (independent of N and λ) with the properties that, for $0 < r < 1$,*

$$\| u_\phi(r,e) - u_\phi^N(r,e) \|^2 \leqq C\chi^*(r). \tag{31}$$

In order to see this, let V_{nj} denote the Fourier constant

$$V_{nj}(r) = \iint_B u_\phi(r,e)S_{nj}(e)\,d\sigma \tag{32}$$

of u_ϕ. Since $d\sigma = \sin\theta\, d\theta d\phi$, a partial integration shows that

$$V_{nj}(r) = -\iint_B u(r,e)S_{nj\,\phi}(e)\,d\sigma. \tag{33}$$

It is clear from (9) that $S_{nj\,\phi} = -jS_{n\,j+n}$ if $j = 0, 1, \cdots, n$ and that $S_{nj\,\phi} = (j-n)S_{n\,j-n}$ if $j = n+1, \cdots, 2n$. Thus

$$V_{nj} = -jU_{n\,j+n} \text{ or } V_{nj} = (j-n)U_{n\,j-n} \tag{34}$$

according as $0 \leqq j \leqq n$ or $n+1 \leqq j \leqq 2n$. The factor j or $j-n$, which is majorized by n, is immaterial (as was the factor $(n+1)^2$ on the right of (28)); so that the proofs of Lemmas 1 and 2 imply Lemma 3.

5. The principal lemmas. Let N be an integer and l a number (not necessarily an integer) subject to the inequalities

$$2 \leqq N \leqq l+2. \tag{35}$$

The estimates to follow will be based on the assumptions that, as $r \to 0$,

$$\| u(r, e) \| = o(r^{N-1}), \tag{36}$$

$$\Phi(r) = o(r^{2l}). \tag{37}$$

These hypotheses, Schwarz's inequality, (10), (11) and (15) show that, as $r \to 0$,

$$| F_{nj}(r) | = o(r^l), \tag{38}$$

$$| U_{nj}(r) | = o(r^{N-1}). \tag{39}$$

Since the last part of (20) is

$$r^{-1-n} \int_0^r s^{n+2} F(s)\, ds = o(r^{l+2}) \text{ as } r \to 0, \tag{40}$$

it follows from $l+2 \geqq N$, (39) and (20) that, as $r \to 0$,

$$I = o(1) \text{ if } n < N, \text{ where } I = I_{nj}(r) = A - \int_r^1 s^{1-n} F(s)\, ds. \tag{41}$$

Thus, if $n < N$,

$$(2n+1)U_{nj}(r) = r^n \int_0^r s^{1-n} F(s)\, ds - r^{-1-n} \int_0^r s^{n+2} F(s)\, ds, \tag{42}$$

where the (conditional) convergence of the first integral is assured by (41).

Schwarz's inequality, as used in obtaining (26) from (25), shows that

$$(2n+1)^2 U^2 \leqq (3-2n+2\mu)^{-1} r^{2\mu+3} \int_0^r s^{-2\mu} F^2(s)\, ds, \tag{43}$$

if (42) holds (for example, if $n < N$) and if $n < \mu + \frac{3}{2}$. Omitting the

factor $(2n+1)^2 \geqq 1$ on the left and summing over $n = 0, 1, \cdots, N-1$ and $j = 0, 1, \cdots, 2n$, it follows that, if $N - 1 < \mu + \frac{3}{2}$,

$$(44_1) \qquad \| u^{N-1} \|^2 \leqq (5 - 2N + 2\mu)^{-1} r^{2\mu+3} \int_0^r s^{-2\mu} \Phi(s)\, ds.$$

Similarly,

$$(44_2) \qquad r^2 \| u_r^{N-1} \|^2 \leqq (5 - 2N + 2\mu)^{-1} r^{2\mu+3} \int_0^r s^{-2\mu} \Phi(s)\, ds,$$

$$(44_3) \qquad \| u_\phi^{N-1} \|^2 \leqq (5 - 2N + 2\mu)^{-1} r^{2\mu+3} \int_0^r s^{-2\mu} \Phi(s)\, ds.$$

For later reference, this result will be stated as a lemma:

LEMMA 4. *Let the conditions on u, f in Lemma 1 hold. In addition, let there exist an integer N and numbers l, μ satisfying (35)-(37) and*

$$(45) \qquad N - 1 < \mu + \tfrac{3}{2} < l + 2.$$

Then (44_1)-(44_3) hold.

It is clear that the convergence of the integral in (44) is implied by (37) and the last part of (45).

It will be convenient to have also the following results on u^N:

LEMMA 5. *Let u, f, l and N satisfy the conditions of Lemma 4. Then, as $r \to 0$,*

$$(46) \qquad \| u^N \| = o(r^{N-\epsilon}) \text{ if } \epsilon > 0.$$

If, in addition, it is supposed that (35) is replaced by

$$(47) \qquad 2 \leqq N < l + 2,$$

then (46) can be improved to

$$(48) \qquad \| u^N - r^N S_N \| = o(r^N),$$

where $S_N = S_N(e)$ is some spherical harmonic of order N.

Since $N \leqq l + 2$, it follows that if $n = N$, then the expression $I = I(r)$ in (41) is $O(|\log r|) = o(r^\epsilon)$ as $r \to 0$, for every $\epsilon > 0$. Hence, by (20) and (40), $U_{nj} = o(r^{n-\epsilon})$ if $n = N$. In view of (44_1), this proves (46).

The last estimate for U_{nj} can be improved to the statement that

$$(49) \qquad \lim_{r \to 0} r^{-n} U_{nj}(r) = B_{nj} \text{ exists if } n = N,$$

provided that $\lim I(r)$ exists (when $n = N$). This is the case, for example, if (47) holds. Hence, if $S_N(e) = \sum_{j=0}^{2N} B_{Nj} S_{Nj}(e)$, then (48) follows from (44_1).

This verification of Lemma 5 and the arguments leading to Lemmas 2 and 3 have the following consequences:

LEMMA 6. *Let the assumptions of Lemma* 4 *hold. Then, as* $r \to 0$,

$$\| u_\phi{}^N \| = o(r^{N-\epsilon}) \text{ if } \epsilon > 0. \tag{50_1}$$

If, in addition, (47) *holds, then*

$$\| u_\phi{}^N - (r^N S_N)_\phi \| = o(r^N). \tag{50_2}$$

LEMMA 7. *Let the assumptions of Lemma* 4 *hold. Then, as* $r \to 0$,

$$r \| u_r{}^N \| = o(r^{N-\epsilon}) \text{ if } \epsilon > 0. \tag{51_1}$$

If, in addition, (47) *holds, then*

$$r \| u_r{}^N - (r^N S_N)_r \| = o(r^N). \tag{51_2}$$

6. $\| u \|$ and $\| \nabla u \|$. The lemmas just proved will be used to obtain estimates for $\| u \|$ and $\| \nabla u \|$ under the assumptions (35) and/or (47), (36) and (37).

In view of (37), the integral in (18) is finite if

$$\lambda + \tfrac{3}{2} < l + 2 \qquad \text{(that is, } \lambda < l + \tfrac{1}{2}\text{)}. \tag{52}$$

Hence, if (16) and (52) hold, then the function in (18) satisfies

$$\chi(r) = O(r^{2\lambda+3}). \tag{53}$$

Then, by (17),

$$\| u - u^N \| = O(r^{\lambda+\frac{3}{2}}) \text{ as } r \to 0. \tag{54}$$

This estimate and (46) imply that, for every $\epsilon > 0$,

$$\| u \| = o(r^{N-\epsilon}) + O(r^{\lambda+\frac{3}{2}}), \tag{55}$$

when (16), (35)-(37) and (52) hold. If, in addition, (47) holds, then

$$\| u - r^N S_N \| = o(r^N) + O(r^{\lambda+\frac{3}{2}}), \tag{55 bis}$$

for some spherical harmonic $S_N = S_N(e)$ of order N.

If, in the arguments leading to (55), (55 bis), Lemmas 1 and 5 are replaced by Lemmas 3 and 6, one obtains

$$\| u_\phi \| = o(r^{N-\epsilon}) + O(r^{\lambda+\frac{3}{2}}), \tag{56}$$

for every $\epsilon > 0$, when (16), (35)-(37) and (52) hold. If, in addition, (47) holds, this can be improved to

$$\| u_\phi - (r^N S_N)_\phi \| = o(r^N) + O(r^{\lambda+\frac{3}{2}}). \tag{56 bis}$$

Similarly, Lemmas 2 and 7 give

$$r \| u_r \| = o(r^{N-\epsilon}) + O(r^{\lambda+\frac{3}{2}}), \tag{57}$$

for every $\epsilon > 0$, when (16), (35)-(37) and (52) hold. If, in addition, (47) holds, then (57) can be improved to

$$r \| u_r - (r^N S_N)_r \| = o(r^N) + O(r^{\lambda+\frac{3}{2}}). \tag{57 bis}$$

It will now be shown that if (16), (35)-(37) and (52) are satisfied, then, for every $\epsilon > 0$,

$$\| \nabla u \| = O(r^{N-1-\epsilon}) + O(r^{\lambda+\frac{1}{2}}). \tag{58}$$

If (35) is strengthened to (47), this can be improved to

$$\| \nabla u - \nabla (r^N S_N(e)) \| = o(r^{N-1}) + O(r^{\lambda+\frac{1}{2}}). \tag{58 bis}$$

To this end, note that

$$ru_r = u_x x + u_y y + u_z z, \tag{59_1}$$

$$u_\phi = -u_x y + u_y x, \tag{59_2}$$

and put

$$u_\psi = u_x z - u_z x. \tag{59_3}$$

It is clear that u_ψ satisfies the same type of inequalities, (56) and/or (56 bis), as u_ϕ. If the equations (59) are solved for u_x, one obtains

$$r^2 u_x = x r u_r - y u_\phi + z u_\psi; \text{ hence } r^2 | u_x |^2 \leqq | ru_r |^2 + | u_\phi |^2 + | u_\psi |^2,$$

by Schwarz's inequality. Thus (56), (57) and the analogue of (56) for u_ψ show that $r \| u_x \| = O(r^{N-1-\epsilon}) + O(r^{\lambda+\frac{3}{2}})$ for every $\epsilon > 0$. A similar estimate holds for $\| u_y \|$ and $\| u_z \|$. Thus (58) follows. The relation (58 bis) is obtained in the same way.

7. Proof of Theorem 1. The partial differential equation (1) can be written as (14), where

$$f = -(a \cdot \nabla u + \gamma u). \tag{60}$$

The assumption (4) and the fact that u is of class C^1 imply that, for $N = 1$, there exists a spherical harmonic S_1 (of order 1) satisfying (3). If $S_1(e) \not\equiv 0$, then the proof of Theorem 1 is complete. If $S_1(e) \equiv 0$, then, for $N = 2$,

$$u = o(r^{N-1}), \qquad \nabla u = o(r^{N-2}). \tag{61}$$

It will be shown that if (61) holds for some integer $N(\geqq 2)$, then there exists a spherical harmonic $S_N(e)$ of order N such that (3) holds, where $S_N(e) \equiv 0$ is not excluded.

In view of (60), the assumption (61) implies that (35)-(37), but not (47), are satisfied when $l = N-2$. Thus, if λ is any number satisfying

$$N = l+2 > \lambda + \tfrac{3}{2} \quad (> \lambda + \tfrac{1}{2}), \tag{62}$$

then the relations (55) and (58) are valid for every $\epsilon > 0$. Let $0 < \epsilon < 1$ and $\lambda + \frac{3}{2} = N - \epsilon$. Then (60), (55) and (58) show that (37) holds if $l = N - 1 - \epsilon$.

Thus, the conditions for (55 bis) and (58 bis) are satisfied if

$$\lambda + \tfrac{3}{2} < l + 2 = N + 1 - \epsilon; \tag{63}$$

cf. (16) and (47). Hence there exists a spherical harmonic S_N of order N satisfying (55 bis). Since $\epsilon > 0$ can be chosen arbitrarily small in (63), this means that

$$\| u(r, e) - r^N S_N(e) \| = o(r^N) \text{ as } r \to 0. \tag{64}$$

Also, (58 bis) gives

$$\| \nabla u(r, e) - \nabla (r^N S_N(e)) \| = o(r^{N-1}) \text{ as } r \to 0. \tag{64 bis}$$

It will be shown that (61) and (64) imply (3). To this end, let $G = G_R(x, \xi)$ denote the Green kernel belonging to Laplace's equation and the boundary condition $u = 0$ on the sphere of radius R. Thus,

$$4\pi G = 4\pi G_R(x, \xi) = |\xi - x|^{-1} - R\,|\xi^* - x|^{-1}\,|\xi|^{-1}, \tag{65}$$

where $\xi^* = R^2\xi/|\xi|^2$ is the image of ξ under inversion of the sphere $|\xi| = R$. Let $P = P_R(x, Re)$ denote the Poisson kernel belonging to the (surface of the) sphere of radius R; so that

$$P = P_R(x, Re) = (4\pi R)^{-1}(R^2 - |x|^2)\,|x - Re|^{-3}. \tag{66}$$

Since $u = u(x)$ is a solution of (14), where $f(x)$ is given by (60), it is seen that, for $r = |x| < R$,

$$u(x) = H_R(x) + v_R(x) \text{ and } \nabla u(x) = \nabla H_R(x) + \nabla v_R(x), \tag{67}$$

where $H_R(x)$ is the harmonic function

$$H_R(x) = \int\!\!\int_B P(x, Re)\, u(Re) R^2 d\sigma \tag{68}$$

and $v_R(x)$ is the particular solution

$$v_R(x) = -\iiint_{|\xi|<R} G(x,\xi) f(\xi)\, d\tau \tag{69}$$

of (14). In (69), $d\tau$ is the element of volume in the sphere $|\xi| < R$.

Since $r^N S_N(e)$ is an harmonic function, it follows that

$$H_R(x) - r^N S_N(x/r) = \iint_B P(x, Re)\{u(Re) - R^N S_N(Re)\} R^2 d\sigma. \tag{70}$$

If $|x| \leqq \frac{1}{2}R$, then $|P(x, Re)R^2| \leqq$ const. Hence, by Schwarz's inequality,

$$|H_R(x) - r^N S_N(x/r)| \leqq \text{Const.} \| u(Re) - R^N S_N(e) \| \text{ if } |x| \leqq \tfrac{1}{2}R.$$

Consequently, (64) shows that, as $R \to 0$,

$$H_R(x) - r^N S_N(x/r) = o(r^N) \text{ uniformly for } |x| \leqq \tfrac{1}{2}R. \tag{71}$$

A similar argument shows that, as $R \to 0$,

$$\nabla H_R(x) - \nabla (r^N S_N(x/r)) = o(r^{N-1}) \text{ uniformly for } |x| \leqq \tfrac{1}{2}R. \tag{72}$$

The assumption (61) shows that the function $f(x)$ in (60) is $o(r^{N-2})$ as $r \to 0$. Hence, by (69),

$$|v_R(x)| = o(R^{N-2}) \iiint_{|\xi|<R} |G(x,\xi)|\, d\tau. \tag{73}$$

The inequality $\iiint_{|\xi|<R} |\xi - x|^{-1} d\tau \leqq 8\pi R^2$, where $|x| \leqq R$, and (65) imply that, as $R \to 0$.

$$v_R(x) = o(R^N) \text{ uniformly for } |x| \leqq \tfrac{1}{2}R. \tag{74}$$

Thus, the first relation in (3) follows from (71), (74) and the first relation in (67).

In order to obtain the asymptotic relation for ∇u in (3), note that

$$|\nabla v_R(x)| = o(R^{N-2}) \iiint_{|\xi|<R} |\nabla G(x,\xi)|\, d\tau; \tag{75}$$

cf. the remark leading to (73). The inequality $\iiint_{|\xi|<R} |\xi - x|^{-2} d\tau \leqq 8\pi R$ and (65) imply that, as $R \to 0$,

$$|\nabla v_R(x)| = o(R^{N-1}) \text{ uniformly for } |x| \leqq \tfrac{1}{2}R. \tag{76}$$

Hence, the assertion in (3) concerning ∇u follows from (67) and (72).

This completes the proof of the fact that (61) implies (3) for some $S_N(e)$. Thus, in order to complete the proof of Theorem 1, it remains to be shown that if $u \not\equiv 0$, then it is impossible that

$$(77) \qquad u = o(r^n), \qquad \nabla u = o(r^{n-1}) \qquad \text{for } n = 0, 1, \cdots.$$

In other words, Corollary 1 remains to be verified (and it is clear, from the result just proved, that there is no loss of generality in strengthening the assumption (7) of Corollary 1 to (77)).

8. Proof of Corollary 1. If l and N are any pair of numbers and if (77) holds, then (36) holds and (37) is a consequence of the definition (60) of f. Let λ be the integer satisfying

$$(78) \qquad \lambda + \tfrac{1}{2} < N < \lambda + \tfrac{3}{2}$$

and let $\mu = \lambda$; so that $2N - 2\lambda - 3 \geqq 1$ and $5 - 2(N+1) + 2\mu \geqq 1$. Then the inequalities (17) in Lemma 1 and (44_1) in Lemma 4, with $N-1$ replaced by N in the latter, are applicable and give

$$(79) \qquad \| u \|^2 \leqq C\{r^{2N} + r^{2\lambda+3} \int_0^1 s^{-2\lambda} \Phi(s)\, ds\},$$

where C is a constant independent of N and λ and depending only on the bounds of u and ∇u.

The inequalities (29), (31) of Lemmas 2, 3 and the inequalities (44_2), (44_3) of Lemma 4, with $N-1$ replaced by N, imply that

$$(80) \qquad \| \nabla u \|^2 \leqq C\{N^2 r^{2N-2}/(1-r^2)^3 + r^{2\lambda+1} \int_0^1 s^{-2\lambda} \Phi(s)\, ds\},$$

by the argument involving (59).

The definition of f in (60) and the relations (79), (80) show that, if a constant c is suitably chosen (depending only on the bounds of u, ∇u, a, γ), then

$$(81) \qquad \Phi(r) \leqq c\{N^2 r^{2N-2}/(1-r^2)^3 + r^{2\lambda+1} \int_0^1 s^{-2\lambda} \Phi(s)\, ds\}.$$

If this inequality is multiplied by $r^{-2\lambda}$, a quadrature gives

$$\int_0^r s^{-2\lambda} \Phi(s)\, ds \leqq c\{N^2 (2N - 2\lambda - 1)^{-1} r^{2N-2\lambda-1}/\epsilon^3 + \tfrac{1}{2} r^2 \int_0^1 e^{-2\lambda} \Phi(s)\, ds\},$$

if $0 \leqq r \leqq (1-\epsilon)^{\frac{1}{2}}$. Thus, $2N-2\lambda-1>2$ implies that

$$(82) \qquad (1-\tfrac{1}{2}cr^2)\int_0^r s^{-2\lambda}\Phi(s)\,ds \leqq c\{N^2r^2/2\epsilon^3+\tfrac{1}{2}r^2\int_r^1 s^{-2\lambda}\Phi(s)\,ds\},$$

if $0 \leqq r \leqq (1-\epsilon)^{\frac{1}{2}}$.

Note that if $f(x)\equiv 0$ in (14), (60), then $u(x)\equiv 0$, for otherwise u is harmonic and satisfies (77). Hence $u(x)\equiv 0$ implies $\Phi(r)\equiv 0$ and conversely.

It will be shown that (77) implies that $u(x)\equiv 0$ on every sphere $|x| \leqq r$ with a radius r satisfying $1-\frac{1}{2}cr^2>0$. Since c is constant, independent of N, λ and depending only on the bounds of u, ∇u, a, γ on $|x| \leqq 1$, it will follow that $u(x)\equiv 0$ on $|x| \leqq 1$.

Suppose, if possible, that $u(x)\not\equiv 0$ on $|x| \leqq r$. Then $\Phi(r)\neq 0$ for some $r=r_0$, where $0 \leqq r_0 < r$. Let $\epsilon>0$ be chosen so that $r \leqq (1-\epsilon)^{\frac{1}{2}}$. Then (82) is applicable. Since $\Phi(r_0)>0$, it follows that the left side of (82) is minorized by const. $r_0^{-2\lambda}$, where const. >0. But the right side is majorized by Const. $(N^2r^2+r^{-2\lambda})$. In view of (78) and $r_0<r$, this leads to a contradiction if $\lambda\to\infty$.

This completes the proof of Corollary 1 and of Theorem 1 (hence of Corollary 2 also).

Part 2. Solutions having a singularity.

9. The nature of the singularity. This part of the paper will deal with functions $u=u(x)$ which are C^1-solutions of (1) on a punctured vicinity of $x=0$, say on

$$(83) \qquad 0<|x| \leqq 1.$$

The theorems to follow will consider the three cases in which the solution $u=u(x)$ satisfies one of the following conditions, as $r=|x|\to 0$:

$$(84) \qquad u(x)=o(1/r),$$

$$(85) \qquad u(x)\to\infty,$$

$$(86) \qquad u(x)=o(r^{-N-2}), \qquad \nabla u(x)=o(r^{-N-3}) \quad \text{for some integer } N \geqq 0.$$

The theorem concerning (84) is a theorem on "removable singularities":

THEOREM 2. *Let x, $\gamma(x)$, $a(x)$ satisfy the conditions of Theorem* 1.

Let $u(x)$ be a C^1-solution of (1) *on* (83) *satisfying* (84) *as* $r \to 0$. *Then $u(0)$ can be defined in such a way that $u(x)$ becomes of class C^1 on* $|x| \leqq 1$.

It will be clear from the proof that the analogue of this theorem is true in the plane. This two-dimensional analogue is an improvement of what follows from the results of [4] on removable singularities, inasmuch as there is no condition on ∇u as $x \to 0$ in Theorem 2. Following Bôcher [1], the theorem on removable singularities is obtained as a consequence of theorems on the existence and uniqueness of a solution having a Green singularity at a given point.

If (84) is replaced by (85), Theorem 2 is altered to

THEOREM 3. *Let x, $\gamma(x)$ satisfy the conditions of Theorem* 1. *Let $u(x)$ be a C^1-solution of* (1) *on* (83) *satisfying* (85), *as* $r \to 0$. *Then there exists a constant $c > 0$ such that, as* $r \to 0$,

$$(87) \qquad u(x) = c/r + O(|\log r|), \qquad \nabla u(x) = \nabla(c/r) + O(1/r).$$

Bôcher [1] has proved theorems similar to Theorems 2 and 3. In his analogue of Theorem 3, the assertion (87) is considerably improved. Bôcher assumes that the coefficient functions a, γ are analytic, but his proof does not use the full force of this assumption. It requires merely that (1) has an adjoint and that both (1) and its adjoint possess Green functions (for some sphere $|x| \leqq R$).

The proof of Theorem 3 will be similar to the proof of its analogue in the plane; cf. [5], pp. 351-352. Note that the assertion of the two-dimensional theorem (*) in [5] is to the effect that $\nabla u = -c\nabla(\log r) + o(1/r)$, but the proof given there shows that this can be improved to

$$\nabla u = -c\nabla(\log r) + O(|\log r|),$$

cf. [5], p. 358.

Theorem 3 is a uniqueness theorem on Green's singularity. There is an existence theorem analogous to the (two-dimensional) theorem (**) in [5], pp. 360-361.

Theorem 2 will depend on Theorem 3, the existence theorem just mentioned and the methods of Part 1 above.

THEOREM 4. *Let x, $\gamma(x)$, $a(x)$ satisfy the conditions of Theorem* 1. *Let $u(x)$ be a C^1-solution of* (1) *on* (83) *satisfying* (86), *as* $r \to 0$. *Then there exists a spherical harmonic $S_N(e)$ of order N (possibly $S_N(e) \equiv 0$) satisfying, as* $r \to 0$,

$$u(x) = r^{-N-1}S_N(e) + o(r^{-N-1}), \quad \nabla u(x) = \nabla(r^{-N-1}S_N(e)) + o(r^{-N-2}),$$

uniformly in e.

The proofs of Theorems 2, 3 and 4 will be applicable if the linear equation (1) is replaced by a non-linear equation (5) for which (6) holds. Although the notation of vector products is used in the proof of Theorem 3, it will be clear that this does not affect the validity of the method if the dimension number 3 is increased.

10. Proof of Theorem 4. The proof is similar to that of Theorem 1 and will only be indicated. Since $U = U_{nj}$ need not be continuous at the origin, (20) must be replaced by

$$(88) \qquad (2n+1)U = r^n\Big(A - \int_r^1 s^{1-n}F(s)\,ds\Big) - r^{-1-n}\Big(B - \int_r^1 s^{n+2}F(s)\,ds\Big),$$

where $A = A_{nj}$, $B = B_{nj}$ are integration constants to be determined. Note that the first part of (86) implies that

$$(89) \qquad U = o(r^{-N-2}) \text{ as } r \to 0.$$

The assumptions (86) imply that f in (14), (60) satisfies

$$(90) \qquad f = o(r^{-N-3}) \text{ as } r \to 0,$$

hence

$$(91) \qquad \Phi = o(r^{-2(N+3)}) \text{ and } F = F_{nj} = o(r^{-N-3}).$$

This estimate of F shows that

$$(92) \qquad r^n \int_r^1 s^{1-n}F(s)\,ds = o(r^{-N-1}) \text{ for } n = 0, 1, \cdots.$$

In fact, the expression on the left is $o(|\log r|)$ or $o(r^{-N-1})$ according as (N, n) is or is not $(-1, 0)$.

In view of (89) and (92), the coefficient of r^{-1-n} in (88) is $o(1)$, as $r \to 0$, if $n > N$; so that

$$(93) \qquad \text{(88) reduces to (20) if } n > N.$$

The (absolute) convergence of the integral which is the factor of r^{-1-n} in (20) is assured by the last part of (91).

It follows that Lemma 1 remains valid if the conditions $\lambda \geqq 0$ and (16) are replaced by

$$(94) \qquad -\tfrac{3}{2} > \lambda > -N - \tfrac{5}{2}$$

and (18) is replaced by

$$\chi(r) = r^{2N+2} + r^{2\lambda+3}(2N+2\lambda+5)^{-1}\int_0^1 s^{-2\lambda}\Phi(s)\,ds. \tag{95}$$

Corresponding analogues of Lemmas 2 and 3 hold.

In order to examine the analogues of the lemmas of Section 5, assume that

$$\Phi(r) = o(r^{-2(l+1)}), \text{ where } l \leqq N+2. \tag{96}$$

This corresponds to (37); the analogue, $\| u(r,e)\| = o(r^{-N-2})$, of (35) is a consequence of (86). It follows that

$$r^{-1-n}\int_r^1 s^{n+2}F(s)\,ds \text{ is } o(r^{1-l}) \text{ or } o(r^{-1-n}|\log r|)$$

according as $n < l-2$ or $n = l-2$. Also

$$\lim_{r\to 0}\Big(B - \int_r^1 s^{n+2}F(s)\,ds\Big) \text{ exists if } n > l-2.$$

Thus, (96) implies that, as $r \to 0$,

$$\| u^N \| = o(r^{-N-1-\epsilon}) \text{ if } N \geqq 0 \text{ and } \epsilon > 0,$$

and this can be improved to

$$\| u^N - r^{-1-N}S_N(e)\| = o(r^{-1-N}) \text{ if } l < N+2,$$

where S_N is some spherical harmonic of order N. These assertions correspond to Lemma 5. It is clear that assertions analogous to Lemmas 6 and 7 hold.

Thus, the arguments in the first part of Section 7 imply the existence of a spherical harmonic S_N of order N satisfying, as $r \to 0$,

$$\| u(x) - r^{-1-N}S_N(e)\| = o(r^{-1-N}), \quad \| \nabla u(x) - \nabla(r^{-1-N}S_N(e))\| = o(r^{-2-N}) \tag{97}$$

if $N \geqq 0$. The proof of Theorem 4 can now be concluded by a modification of the arguments of the second part of Section 7. The Green kernel (65) of the sphere $|x| \leqq R$ must be replaced by the Green kernel of a region of the type $R/4 \leqq |x| \leqq 4R$, and the Poisson kernel (66) by the kernel used to determine an harmonic function on $R/4 < |x| < 4R$ when its values on the two concentric spheres $|x| = R/4$ and $|x| = 4R$ are given; cf., e. g., [3]. The analogues of (71), (72), (74), (76), when $|x| \leqq \frac{1}{2}R$ is replaced by $\frac{1}{2}R \leqq |x| \leqq 2R$, can then be deduced.

11. Proof of Theorem 3. The proof will be similar to the proof for the analogous theorem in the plane; cf. [5]. Assume first that

$$\gamma(x) \equiv 0 \tag{98}$$

in (1). Then, by Theorem 1, the zeros of the gradient of u can cluster only at $x = 0$, since (98) shows that Corollary 2 of Theorem 1 is applicable to $u(x) - u(x_0)$ at any point $x = x_0$ of (83). It follows, by arguing as in [5], p. 355, that there exist arbitrarily large constants C such that the locus

$$L = L_C\colon\ u(x) = C \tag{99}$$

is a closed (Jordan) C^1-surface surrounding $x = 0$. Furthermore,

$$u_p = p \cdot \nabla u \geqq 0 \text{ on } L, \tag{100}$$

where p is the inward unit normal vector to L (and u_p is, therefore, the corresponding normal derivative of u).

If T is a suitable region bounded by a surface S and p is the unit outward normal on S, finally v is a suitable scalar function, then Green's identity is

$$\iint_S v \nabla u \cdot p dS = \iiint_T (v \Delta u + \nabla v \cdot \nabla u) dT. \tag{101}$$

Also, if w is a smooth vector function, Green's identity gives

$$\iint_S (w \times \nabla u) \cdot p dS = \iiint_T \nabla u \cdot (\nabla \times w) dT,$$

where $\times$ denotes vector multiplication. If the second of these relations is subtracted from the first, one obtains

$$\iint_S \nabla u \cdot (vp + (w \times p)) dS = \iiint_T v \Delta u dT, \tag{102}$$

provided that

$$\nabla \times w = \nabla v.$$

For a given v, the last equation has a solution w if and only if v is harmonic. If u is a C^1-solution of a Poisson equation (14) and if S and w are sufficiently smooth, then (102) remains valid.

Let ξ be a 3-dimensional vector and let $x - \xi$ have the components (X, Y, Z). Choose

$$v = X/\rho^3, \text{ where } \rho = |x - \xi| \tag{103}$$

(so that v is the first component of $-\nabla(1/\rho)$). A vector w satisfying the equation following (102) is

$$w = (0,\ Z/\rho^3,\ -Y/\rho^3). \tag{104}$$

Apply the relation (102) to the region T bounded by the sphere B: $|\xi| = 1$, the locus (99) and a small sphere $|x-\xi| = \epsilon$ about a fixed point x (between B and L). On the sphere $|x-\xi| = \epsilon$, the outward unit normal p is $(x-\xi)/\epsilon$. Hence, $vp + (w \times p) = (1/\epsilon^2, 0, 0)$, and so

$$\lim_{\epsilon \to 0} \iint_{|x-\xi|=\epsilon} \nabla u \cdot (vp + (w \times p))\, dS = 4\pi u_x(x)$$

(here $u_x = \partial u/\partial x$ is the first component of ∇u). Also, note that $\nabla u \cdot (w \times p) = 0$ on L. Hence (102)-(104) lead to

$$4\pi u_x(x) = \tag{105_x}$$

$$-\iint_L v u_p\, dS + \iint_B \nabla u \cdot (vp + (w \times p))\, d\sigma - \iiint_T v \Delta u\, d\tau,$$

where $T = T(C)$ is the region bounded by B and $L = L_C$.

The relations (105_x), the corresponding relations (105_y), (105_z) for $u_y(x)$, $u_y(x)$ and Green's identity

$$\iint_L u_p\, dS = -\iint_B u_p\, d\sigma + \iiint_T \Delta u\, d\tau \tag{106}$$

are the exact analogues of formulae (22), (28) used in [5] for the proof of the planar case of Theorem 3 (when (98) is assumed). A modification of the arguments of [5], pp. 356-357, leads to the result that

$$4\pi c = \lim_{C \to \infty} \iint_L u_p\, dS \text{ exists} \tag{107}$$

and to the asymptotic relation

$$\nabla u = c\nabla(1/r) + O(1/r) \text{ as } r \to 0. \tag{108}$$

The relation (108) and a quadrature of (108) give Theorem 3, in the case (98). Finally, the general case can be reduced to (98) by a variation of constants; cf. [5], pp. 359-360.

12. Proof of Theorem 2. The existence theorem mentioned after Theorem 3 is to the effect that if $R > 0$ is sufficiently small, then (1)

has a C^1-solution $u = G(x)$ on $0 < |x| \leqq R$ satisfying $G(x) \to \infty$ as $x \to 0$. By Theorem 3,

$$G(x) = c/r + O(|\log r|), \qquad \nabla G(x) = \nabla(c/r) + O(1/r),$$

as $r \to 0$, where $c > 0$.

If (84) holds, then $u(x) + G(x)$ is a C^1-solution of (1) on $0 < |x| \leqq R$ satisfying $u(x) + G(x) \to \infty$ as $x \to 0$. It follows from Theorem 3. (84) and the last formula line that

$$u(x) = O(|\log r|), \qquad \nabla u(x) = O(1/r), \tag{109}$$

as $r \to 0$. Thus

$$U = U_{nj} = O(|\log r|), \tag{110}$$

$$\Phi = O(r^{-2}) \text{ and } F = F_{nj} = O(r^{-1}). \tag{111}$$

One of the terms on the right of (88) is

$$-r^n \int_r^1 s^{1-n} F(s)\, ds = O(1),\ O(r|\log r|) \text{ or } O(r) \tag{112}$$

according as $n = 0$, $n = 1$ or $n > 1$. In view of (110), the coefficient of r^{-1-n} in (88) is $o(1)$ as $r \to 0$. Hence

$$B - \int_r^1 s^{n+2} F(s)\, ds = \int_0^r s^{n+2} F(s)\, ds,$$

where the absolute convergence of the last integral is assured by (111). Thus

(113) (88) reduces to (20) if $n \geqq 0$.

Analogues of the Lemmas 1-3 give $\| u - u^0 \|^2 = O(r^2 + r^{2\lambda+3})$ if $\lambda < -\frac{1}{2}$. The case $n = 0$ of (20) and the estimate for F in (111) show that $U_{00} = \text{Const.} + O(r)$. Hence $\| u - \text{Const.} \| = O(r)$ as $r \to 0$.

The proof of Theorem 2 can now be completed along the lines used to prove Theorem 1. In fact, the proof of

$$u(r, e) - \text{Const.} = O(r)$$

is identical with the proof of the first formula of (3) in Theorem 1; cf. the derivation of (71), (74). The analogue of (72), namely, $\nabla H_R(x) = O(1)$ uniformly for $|x| \leqq \frac{1}{2}R$, is clearly valid. In order to obtain the analogue of (76), namely, $\nabla v_R(x) = O(1)$ uniformly for $|x| \leqq \frac{1}{2}R$, replace (75) by $|\nabla v_R(x)| \leqq I_1 + I_2$, where I_1, I_2 are the integrals of $|\nabla G(x, \xi)|\,|\nabla u|$ over

the domains $|\xi| \leqq R/4$ and $R/4 \leqq |\xi| \leqq R$, and let $|x| = \frac{1}{2}R$. Then, since $|\nabla u| = O(1/r)$, by (1) and (109),

$$I_1 = O(R^{-2}) \int\int\int |\xi|^{-1} d\tau = O(1),$$

$$I_2 = O(R^{-1}) \int\int\int |x-\xi|^{-2} d\tau = O(1).$$

Consequently, $|\nabla u(x)| = O(1)$ as $|x| = \frac{1}{2}R \to 0$. Thus $f(x)$ in (14), (60) is bounded. From this, it follows that $u(x)$ is of class C^1 (at $x = 0$ also). This proves Theorem 2.

THE JOHNS HOPKINS UNIVERSITY.

REFERENCES.

[1] M. Bôcher, "Singular points of functions which satisfy partial differential equations of the elliptic type," *Bulletin of the American Mathematical Society*, vol. 9 (1903), pp. 455-465.

[2] T. Carleman, "Sur les systèmes linéaires aux dérivées partielles du premier ordre à deux variables," *Comptes Rendus*, vol. 197 (1933), pp. 471-474.

[3] U. Dini, "Il problema di Dirichlet in un'area anulare, e nello spazio compreso fra due sfere concentriche," *Rendiconti del Circolo Matematico di Palermo*, vol. 16 (1913), pp. 1-28.

[4] P. Hartman and A. Wintner, "On the local behavior of solutions of non-parabolic partial differential equations," *American Journal of Mathematics*, vol. 75 (1953), pp. 449-476.

[5] ——— and A. Wintner, "On the local behavior of solutions of non-parabolic partial differential equations. II. The uniqueness of the Green singularity," *ibid.*, vol. 76 (1954), pp. 351-361.

[6] C. Müller, "On the behavior of the solutions of the differential equations $\Delta U = F(x, U)$ in the neighborhood of a point," *Communications on Pure and Applied Mathematics*, vol. 7 (1954), pp. 505-516.

ON THE ASSIGNMENT OF ASYMPTOTIC VALUES FOR THE SOLUTIONS OF LINEAR DIFFERENTIAL EQUATIONS OF SECOND ORDER.*

By PHILIP HARTMAN and AUREL WINTNER.

Let both coefficients of the homogeneous, linear differential equations

$$x'' + g(t)x' + f(t)x = 0 \tag{1}$$

be given as continuous functions for large positive t.

Suppose that, corresponding to every given value, c, the differential equation (1) has a unique solution $x = x(t)$ satisfying

$$x \to c \tag{2}$$

as $t \to \infty$ (so that $x(\infty)$ can be assigned as an "initial condition" and this single integration constant determines the solution $x(t)$ uniquely, even though (1) is of second order). Then (1) will be called *of type* (*). Clearly, (1) is of type (*) if and only if (1) has exactly one solution satisfying the case $c = 1$ of (2) and, in addition, the case $c = 0$ of (2) is satisfied only by the trivial solution ($\equiv 0$). It is also clear that, since the general solution of (1) contains two arbitrary constants, $x(\infty)$ cannot exist (as a finite limit) for all solutions $x(t)$, if (1) is of type (*).

If $x(\infty)$ exists (as a finite limit) for all solutions and if $x(\infty) \neq 0$ holds for some solution, then (1) will be called *of type* (**). Clearly, this will be the case if and only if there exist a solution satisfying the case $c = 1$ of (2) and a non-trivial solution ($\not\equiv 0$) satisfying the case $c = 0$ of (2). By adding to the former any constant multiple of the latter, it is seen that (1) is of type (**) if and only if there belongs to some and/or every $c \neq 0$ two, linearly independent, solutions $x(t)$ satisfying (2).

The following theorem will first be proved:

(I) *In order that* (1) *be of type* (*), *it is sufficient that*

(i) *the coefficient functions of* (1) *satisfy the conditions*

$$(3_1) \qquad \int^{\infty} t\,|f(t)|\,dt < \infty, \qquad\qquad (3_2) \qquad g(t) \leqq 0,$$

and it is also sufficient that

* Received January 3, 1955.

(ii) *condition* (3_1) *of* (i) *be reduced, but condition* (3_2) *of* (i) *be strengthened, as follows:*

$$(4_1) \qquad \int^{\infty} |f(t)|\,dt < \infty, \qquad (4_2) \qquad g(t) \leqq \text{const.} < 0.$$

Condition (3_1) of (i) cannot be relaxed to (4_1) if (4_2) is relaxed to (3_2), as in (i). Otherwise it would follow that (1) is of type (*) whenever (4_1) holds and $g(t) \equiv 0$. But this is not true. In fact, it is known that if $f(t)$ is real-valued and does not change sign, then (3_1) is not only sufficient (Bôcher) but necessary (Weyl) as well in order that the case $g(t) \equiv 0$ of (1) be of type (*) (for a simple proof, cf. [6]).

It will be clear from the proof of part (i) of (I) that the assumption (3_2) of (i) can be generalized to

$$(5) \qquad \int^{\infty} g^+(t)\,dt < \infty, \quad \text{where } g^+ = \max(0, g);$$

so that (3_1) and (5) (hence either (3_1) and $\int^{\infty} |g(t)|\,dt < \infty$ or (3_1) and (3_2)) are sufficient in order that (1) be of type (*). Note that g (but not f) is here assumed to be real-valued; cf. the remark preceding the proof of (I) below.

The proof will show that, under the conditions of (I), it is possible to assert much more than the fact that (1) is of type (*). As will be seen from the proof of (I), condition (3) or (4) implies that (1) has a pair of linearly independent solutions $x = x_1(t)$, $x_2(t)$ satisfying, as $t \to \infty$,

$$x_1(t) \to 1, \quad x_1' = o(1/s); \qquad x_1(t) \sim s, \quad x_2' \sim \mu,$$

where $\mu = \mu(t)$ and $s = s(t)$ are defined by (10) and (11) below.

A simple illustration of part (ii) of (I) is the following known fact: Whenever (4_1) is satisfied,

$$(6) \qquad z'' - \{1 + f(t)\}z = 0$$

has a (unique) solution $z(t)$ which is asymptotically equal to e^{-t}, that is, for which the function $x(t) = e^t z(t)$ satisfies the case $c = 1$ of (2). In order to see this, it is sufficient to observe that substitution of $z = e^{-t}x$ into (6) leads to the case $g(t) \equiv -2$ of (1); so that part (ii) of (I) becomes applicable.

A criterion which belongs to property (**) in the same way as part (ii) of (I) belongs to property (*) is as follows:

(II) *In order that* (1) *be of type* (**), *it is sufficient that the coefficient functions of* (1) *satisfy the conditions*

$$(7_1) \qquad \int^{\infty} |f(t)dt < \infty, \qquad (7_2) \qquad \operatorname{Re} g(t) \geqq \text{const.} > 0.$$

Note that, while (7_1) is identical with (4_1), condition (7_2) is a dual of condition (4_2), if $g(t)$ is real-valued (which is not assumed in (II)). Since (II) corresponds to part (ii) of (I), it is worth mentioning that what would correspond to part (i) of (I) as a (**)-criterion is false. In other words, (3_1) and $g(t) \geqq 0$ together fail to assure that (1) is of type (**). This is seen by choosing $f(t) \equiv 0$ and $g(t) \equiv 0$.

It should also be remarked that (I) becomes false if $g(t)$ is allowed to be complex-valued and $g(t)$ is replaced by $\operatorname{Re} g(t)$ in (3_2) and/or (4_2). In order to see this, consider the case $f(t) \equiv 0$ of (1) (so that f satisfies (3_1)). The general solution of the corresponding differential equation (1) is $c_1 + c_2 s(t)$, where c_1, c_2 are arbitrary constants and $s(t)$ is defined by (10), (11) below. Thus the desired example results if $\operatorname{Re} g(t) = -1$ and $s(\infty) = \lim s(t)$ exists as a finite limit (for, in this case, (1) is of type (**), not (*)). If $g(t) = -(1 + ite^t)$, then

$$s(t) = \int^{t} \mu(u)du \text{ and } \mu(u) = e^u \exp i \int^{u} ve^v dv.$$

Define $w = w(u) = \int^{u} ve^v dv$, so that $e^u du = dw/u$. The change of integration variables $u \to w$ gives for $s(t)$ the formula

$$s(t) = \int^{w(t)} (e^{iw}/u(w))dw,$$

where $u = u(w)$ is the inverse of $w = w(u)$. It is clear that $w(t) \to \infty$ as $t \to \infty$ and that $1/u(w)$ tends monotonously to 0 as $w \to \infty$. Hence $s(\infty)$ exists (as a finite limit). Thus the case $f \equiv 0$, $g = -(1 + ite^t)$ of (1) is not of class (*).

Proof of (I). It is known that, if $h(s)$ is defined and continuous for large positive s, then the condition

$$(8) \qquad \int^{\infty} s\,|h(s)|\,ds < \infty$$

(and even a somewhat weaker assumption; cf. [5], [3]) is sufficient in order that the differential equation

$$\ddot{x} + h(s)x = 0, \tag{9}$$

where $\dot{x} = dx/ds$, has two solutions, say $x = x_1(s)$ and $x = x_2(s)$, satisfying $x_1(s) \to 1$, $x_2(s) \sim s$ (and $\dot{x}_1 = o(1/s)$, $\dot{x}_2 \to 1$) as $s \to \infty$. Hence (8) is sufficient in order that (9) be of type (*). Both assertions of (I) will be reduced to this fact.

First, whether (4_2) or just (3_2) is assumed, it is clear that $\mu = \mu(t)$, where

$$\mu = \exp - \int^t g(u)\, du, \tag{10}$$

is a positive function, hence $s = s(t)$, where

$$ds = \mu dt, \tag{11}$$

is an increasing function, and that $s \to \infty$ as $t \to \infty$ (the choice of the integration constants in (10) and (11) will be immaterial). On the other hand, if the independent variable t is replaced by s in (1), it is readily verified from (10) and (11) that (1), where $x' = dx/dt$, goes over into (9), where $\dot{x} = dx/ds$ and

$$h = f/\mu^2. \tag{12}$$

Since (8) implies that (9) is of type (*), it follows that (1) will be proved to be of type (*) if it is shown that, whether (3_1) and (3_2) or (4_1) and (4_2) are assumed, the function (12) of s will satisfy (8). Since $s = \infty$ corresponds to $t = \infty$, this requires that

$$\int^\infty s(t)\,|f(t)|/\mu^2(t)ds(t) < \infty$$

or, what in view of (11) and (10) is the same thing, that

$$\int^\infty |f(t)|\,(\int^t \mu(v)dv)/\mu(t)dt < \infty. \tag{13}$$

Ad (i). It is clear from (3_2) and (10) that $\mu(t)$ increases with t. This implies that the indefinite integral of $\mu(t)$ is majorized by a constant multiple of $t\mu(t)$. Hence (13) follows from (3_1).

Ad (ii). If only (4_1) is assumed, (13) will hold if the quotient

$$(\int^t \mu(v)dv)/\mu(t) \tag{14}$$

is bounded as $t \to \infty$. On the other hand, in view of an applicable "O-variant" of l'Hôpital's rule, (14) will be bounded if the quotient $\mu(t)/\mu'(t)$ is. But (10) shows that the latter quotient is identical with the function $-1/g(t)$. Finally, the boundedness of this function is assured by (4_2).

Proof of (II). It is known ([4], pp. 55-56) that if $p(t) \neq 0$ and $q(t)$ are, for large positive t, continuous functions satisfying the pair of conditions

$$(15_1) \quad \int^{\infty} |p(t)|^{-1}\, dt < \infty, \qquad (15_2) \quad \int^{\infty} |q(t)| \Big(\int_t^{\infty} |p(u)|^{-1}\, du \Big) dt < \infty,$$

then the differential equation

$$(16) \qquad (p(t)x')' + q(t)x = 0$$

has a pair of linearly independent solutions, say $x = x_1(t)$ and $x = x_2(t)$, satisfying $x_1(t) \to 1$ and $x_2(t) \to 0$ as $t \to \infty$. This means that (15_1) and (15_2), where $p(t) \neq 0$, imply that (16) is of type (**).

On the other hand, if (1) is multiplied by the (non-vanishing) function $e^{j(t)}$, where

$$(17) \qquad j(t) = \int^{t} g(u)\, du,$$

then (1) appears in the form (16), where

$$(18_1) \quad p(t) = e^{j(t)}, \qquad (18_2) \quad q(t) = f(t) e^{j(t)}.$$

Hence (II) will be proved if it is shown that (7_1) and (7_2) imply (15_1) and (15_2) by virtue of (17)-(18_2); in other words, that

$$(19_1) \qquad \int^{\infty} |e^{-j(t)}|\, dt < \infty,$$

$$(19_2) \qquad \int^{\infty} |f(t) e^{j(t)}| \Big(\int_t^{\infty} |e^{-j(u)}|\, du \Big) dt < \infty.$$

If $c > 0$ denotes the constant occurring in (7_2), it is clear from (17) that $|e^{-j(t)}|$ is majorized by a constant multiple of e^{-ct}, which implies that (19_1) is satisfied. But it is also seen from (7_2) and (17) that

$$\int_t^{\infty} |e^{-j(u)}|\, du \leqq c^{-1} \int_t^{\infty} |\operatorname{Re} g(u)|\, |e^{-j(u)}|\, du \leqq c^{-1} |e^{-j(t)}|.$$

Hence (19_2) is satisfied if $\int^{\infty} |f(t)e^{j(t)}|\,|c^{-1}|\,|e^{-j(t)}|\,dt<\infty$ is, that is, if (7_1) is.

A theorem of somewhat different nature will now be considered.

(III) *In the differential equation*

$$z''+f(t)z=0, \tag{20}$$

let $f(t)$, where $0\leqq t<\infty$, be a complex-valued, continuous function having a non-positive real part. Then (20) has a solution $z(t)\neq 0$ corresponding to which $|z(t)|^2$ is a non-increasing, convex function on $0\leqq t<\infty$. In particular, the limit of $|z(t)|$ as $t\to\infty$ exists as a finite limit $(\geqq 0)$. Any solution $z=w(t)$ of (20) linearly independent of this solution $z(t)$ is subject to the condition $|w(t)|\to\infty$ as $t\to\infty$.

If $f(t)$ is real-valued, then (III) reduces to a well known theorem of A. Kneser. In order to prove (III), let $z=x+iy$ and $f(t)=a(t)+ib(t)$. Then (20) can be written as a real system,

$$\begin{pmatrix} x'' \\ y'' \end{pmatrix}+F(t)\begin{pmatrix} x \\ y \end{pmatrix}=0, \text{ where } F=\begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

Since $a\leqq 0$ by assumption, the symmetric part of the matrix F is non-positive definite. Hence (III) can be concluded from a result of [5].

Appendix.

When confined to the real field, both (I) and (II) refer to cases in which (1) is non-oscillatory (cf. below). This Appendix deals with the general class of non-oscillatory differential equations (1) under the assumption that the x'-term is absent from (1).

For large positive t, let $f(t)$ be a real-valued, continuous function, and consider only those solutions $x(t)$ of the differential equation

$$x''+f(t)x=0 \tag{1}$$

which are real-valued and distinct from the trivial solution $(\not\equiv 0)$. Thus, since the values of x and x' at a given t determine a solution of (1) uniquely, x and x' cannot vanish simultaneously, and so $x(t)$ must change sign wherever it vanishes. If there exists a particular solution $x(t)$ which does not vanish for large t, say for $t_0\leqq t<\infty$, then (1) is called non-oscillatory, and otherwise oscillatory. This classification of the differential equations (1) is inde-

pendent of the choice of the particular solution $x(t)$, since, in view of Sturm's separation theorem, every solution of (1) must have zeros clustering at $t=\infty$ if one solution has such zeros.

If (1) is non-oscillatory, then, for reasons which will be apparent from the results to be proved below, a solution $x(t)$ of (1) will be called *principal* or *non-principal* according as the (continuous) function $1/x(t)$ is not or is of class L^2 on the half-line $[t_0, \infty)$ when t_0 is large enough (namely, larger than the last zero of $x(t)$).

If $x(t)$ is a non-principal solution, that is, if the second factor of the product

$$x(t)\int_t^\infty (x(s))^{-2}\,ds \tag{2}$$

can be formed (for $t \geqq t_0$), then two differeniations of the product show that the function (2) is a solution of (1), since $x(t)$ is. These two solutions are linearly independent, since their ratio is not a constant. Actually, the solution (2) can be obtained by solving for $y=y(t)$ the case $c=-1$ of the differential relation (3) below.

Let $x=x(t)$ and $x=y(t)$ be any two solutions of (1). Then their Wronskian is a constant,

$$xy'-yx'=c, \tag{3}$$

and the constant c is distinct from 0 if and only if the two solutions are linearly independent. Suppose that they are, that (1) is non-oscillatory, and that t is large enough. Then (3) can be written, on the one hand, as

$$(\log y)'-(\log x)'=c/(xy), \quad \text{where } c\neq 0, \tag{4}$$

and, on the other hand, as

$$(y/x)'=c/x^2, \quad \text{where } c\neq 0. \tag{5}$$

With the aid of these formulations of (3) (and of its formulation (2), specified above), the following theorem will be proved:

THEOREM. *If* (1) *is non-oscillatory, then it has a principal solution, and the latter is unique to an arbitrary constant factor* ($\neq 0$).

This contains the following corollary (which corollary of the theorem will, however, be needed in the proof of the theorem):

COROLLARY. *If* (1) *is non-oscillatory, then one (at least) of any two of its linearly independent solutions is non-principal.*

This, in turn, implies the existence of a non-principal solution. A proof for the existence of such a solution is between the lines of [1], p. 703 (and the properties of non-principal solutions are further analyzed in [2], p. 633). The following proof of the Corollary is a simplification of the proof just mentioned.

Let $x(t)$ and $y(t)$ be the two solutions referred to in the Corollary. Then, since (5) holds for large t, the function $y(t)/x(t)$ is ultimately monotone. Hence

$$y(t)/x(t) \to C, \quad \text{as } t \to \infty, \tag{6}$$

holds for some limit C, provided that $C = \infty$ and $C = -\infty$ are allowed. The latter two possibilities can, however, be reduced to the case $C = 0$, since $x(t)$ and $y(t)$ can be interchanged. But if (6) holds for some finite C, then it is seen from (5) that an indefinite integral of the square of $1/x(t)$ must tend to a finite limit as $t \to \infty$. Since this means that $x(t)$ is non-principal, the assertion of the Corollary follows.

Besides the Corollary, part of the following Lemma will be needed in the proof of the Theorem.

LEMMA. *If* (1) *is non-oscillatory and if* $x(t)$ *is a fixed non-principal solution of* (1), *then every solution of* (1) *is of the form*

$$Cx(t) + o(|x(t)|), \qquad \text{as } t \to \infty, \tag{7}$$

where the constant C *is or is not* 0 *according as the solution* (7) *is principal or non-principal.*

In order to prove this, suppose that $y(t)$ is a non-principal solution. Then, since $x(t)$ is supposed to be non-principal, and since the product of two functions of class L^2 is of class L, it follows from (4) that $\log y - \log x$ tends to a finite limit as $t \to \infty$, which means that (6) holds for a finite $C \neq 0$. This proves that assertion of the Lemma which concerns the case $C \neq 0$ of (7). In the remaining case, the assertion of (7) is that every principal solution must be $o(|x(t)|)$ if $x(t)$ is non-principal.

If $x(t)$ is non-principal, then the solution (2) exists (for large t) and is of the form $x(t)o(1)$, which is $o(|x(t)|)$. Hence, by that part of the Lemma which has already been proved, the solution (2) cannot be non-principal. Consequently, the proof of the Lemma as well as the proof of the Theorem will be complete if it is assured that there cannot exist two linearly independent solutions both of which are principal. But this is assured by the Corollary.

REMARK. (*Added* 4.8.1955). The notion of a principal solution has a curious application to the general case of (1), the case in which $f(t)$ is real-valued and continuous for large positive t but (1) is not required to be non-oscillatory.

First, it is easily verified from (3), (1) and the case $x = y$ of (1) that $r = (x^2 + y^2)^{\frac{1}{2}} > 0$ is a solution of

$$r'' + g(t)r = 0, \tag{8}$$

where $g(t) = f(t) - c^2/r^4(t)$, $c^2 > 0$. Since $r = r(t)$ is positive throughout, (8) is non-oscillatory and has therefore both principal and non-principal solutions. To which of these two types will the particular solution $r = (x^2 + y^2)^{\frac{1}{2}}$ belong? The answer turns out to be as follows: *$r = (x^2 + y^2)^{\frac{1}{2}}$ is a non-principal or principal solution of* (8) *according as* (1) *is not or is non-oscillatory.*

In order to see this, consider the complex-valued solution $z = x + iy$ of (1). Then $z \neq 0$ and $z' \neq 0$, by (3), where $c \neq 0$, and it is also seen that the imaginary part of z'/z is c/r^2, where $r = |z|$. Hence $(\arg z)' = c/r^2$. This implies that $\arg(x + iy)$ is a strictly monotone function of t and that $1/r(t)$ is of class L^2 if and only if $\arg(x + iy)$ is bounded as $t \to \infty$. Since the latter condition is satisfied if and only if x (and/or y) fails to acquire an infinity of zeros as $t \to \infty$, it follows that $1/r(t)$ is of class L^2 if and only if (1) is non-oscillatory. This proves the last italicized statement.

THE JOHNS HOPKINS UNIVERSITY.

REFERENCES.

[1] P. Hartman, "Differential equations with non-oscillatory eigenfunctions," *Duke Mathematical Journal*, vol. 15 (1948), pp. 697-709.

[2] ——— and A. Wintner, "Oscillatory and non-oscillatory linear differential equations," *American Journal of Mathematics*, vol. 71 (1949), pp. 627-649.

[3] ——— and A. Wintner, "On non-oscillatory linear differential equations," *ibid.*, vol. 75 (1953), pp. 717-730.

[4] A. Wintner, "Asymptotic integrations of the adiabatic oscillator in its hyperbolic range," *Duke Mathematical Journal*, vol. 15 (1948), pp. 55-67.

[5] ———, "On linear repulsive forces," *American Journal of Mathematics*, vol. 71 (1949), pp. 362-366.

[6] ———, "On almost free linear motions," *ibid.*, vol. 71 (1949), pp. 595-602.

MAJORANTS IN SPACES OF INTEGRABLE FUNCTIONS.*[1]

By G. G. LORENTZ.

1. Introduction. Let $f(x)$ denote an integrable function on the interval $(0,1)$. The Hardy-Littlewood majorant of $f(x)$ is the function

$$\theta(x) = \theta(x;f) = \sup_y \int_x^y f(t)\,dt/(y-x), \tag{1}$$

provided it exists almost everywhere (a.e.). Hardy and Littlewood have shown (see for example [5], p. 244) that if $f \in L^p$, then $\theta(f)$ is defined and also belongs to L^p. More generally, if X is a certain space of integrable functions over $(0,1)$, we shall say that X has the *Hardy-Littlewood property* (or shortly that $X \in \mathrm{HLP}$) if $f \in X$ always implies $\theta(f) \in X$. The most general spaces X which we shall consider are the Köthe-Toeplitz spaces $X(C)$ defined as follows (compare [3]). Let C be some class of integrable non-negative functions $c(x)$ on $(0,1)$, which contains a function greater than a positive constant. A function $f(x)$ belongs to $X(C)$ and has norm $\|f\|$ if

$$\|f\| = \sup_{c \in C} \int_0^1 |f(x)|\,c(x)\,dx < +\infty. \tag{2}$$

$X(C)$ is a Banach space [3]; its dual X' is the space of all integrable functions g such that $\int_0^1 fg\,dx$ exists for all $f \in X$. In this case the suprema of $\int_0^1 fg\,dx$ for all f with $\|f\| \leqq 1$ and of $\int_0^1 f|g|\,dx$ for all $f \geqq 0$ with $\|f\| \leqq 1$ are equal and finite, and by definition equal to the norm of g in X'. Thus our "dual space of X" is different from "conjugate space of X" in Banach's terminology (i.e. the space of all bounded linear functionals on X). The use of dual spaces rather than conjugate spaces is justified by the fact that the former are simpler and that the second dual of X may be X even if X is not reflexive. Actually, the relation $X'' = X$ holds for any Köthe-Toeplitz space.

The importance of Köthe-Toeplitz spaces is underlined by the fact that they are identical (as has been shown by the author in a paper under prepara-

* Received December 2, 1954.

[1] This work was supported by the research grant NSF G 1014 at Wayne University, sponsored by the National Science Foundation.

tion for publication) to an apparently more general class of spaces ([2], p. 415) described in terms of lattice operations in X and the norm $\|f\|$ only, without reference to the class $C=\{c\}$. Essentially identical with these are spaces discussed by Ellis and Halperin [6], p. 576.

Our problem will be to give necessary and sufficient conditions for C in order that a Köthe-Toeplitz space $X(C)$ should have the Hardy-Littlewood property.

We shall assume that C is *rearrangement-invariant*, that is, with each $c(x)$ any of its rearrangements [3] $c_r(x)$ also belong to C. (Then $X(C)$ will also be rearrangement-invariant.) In this case the answer is easily given (see Section 2): for each $c \in C$, the function

$$\bar{c}(x)=\int_x^1 v(t)/t\,dt \tag{3}$$

should belong to X'.

Special cases of spaces $X(C)$ with rearrangement-invariant C are spaces $\Lambda(\phi)$, $M(\phi)$ [3] and Orlicz spaces L_Φ (for an exposition of the theory of Orlicz spaces see [4]). Here the condition just given may be simplified so as to bear directly on ϕ or Φ. This is carried out in Sections 3-5. Spaces $\Lambda(\phi, p)$ and $M(\phi, p)$ (see [3]), with $p>1$, are not very interesting in our problem, since the original argument of Hardy and Littlewood is sufficient to show ([1], [2]) that they have the Hardy-Littlewood property.

The importance of the Hardy-Littlewood property lies in the fact that it is equivalent to the *dominated convergence* a.e. of the quotients $f_h(x)=h^{-1}\{F(x+h)-F(x)\}$, where $F(x)$ is the indefinite integral of $f(x)$, to the latter function, whenever $f(x)$ lies in X, the common majorant for the f_h being $\theta(x;f)$. In lattice-theoretic terms, this dominated convergence may be shown to be equivalent to the *order convergence* of f_h to f in the Banach lattice X endowed with its natural partial order. The dominated convergence of f_h to f implies dominated convergence to f of many types of singular integrals; for example, the Fejér and Poisson integrals (compare [5], p. 247). These facts justify our interest in the Hardy-Littlewood property.

2. Hardy-Littlewood property of the spaces $X(C)$. For a positive and decreasing function $f(x)$, the majorant $\theta(x;f)$ is obviously equal to the function

$$\tilde{f}(x)=\int_0^x f(t)\,dt/x. \tag{4}$$

It is therefore natural to consider the properties of a space $X(C)$, which

we call HLP′ and HLP″, defined by the requirements that $\tilde{f} \in X(C)$ for all $f \in X(C)$ or that $\tilde{f} \in X(C)$ for all positive decreasing f in $X(C)$.

Since $\tilde{f}(x)$ is contained between $\theta(x;f)$ and

$$-\theta(x;-f) = \inf_y \int_y^x f(t)\,dt/(y-x),$$

it is clear that HLP implies HLP′, and this in turn implies HLP″.

LEMMA. *If C is rearrangement-invariant, then all properties* HLP, HLP′, HLP″ *are equivalent, and each implies*

$$(5) \qquad \|\theta(f)\| \leqq A\|f\| \quad \textit{and} \quad (6) \qquad \|\tilde{f}\| \leqq A\|f\|$$

with some constant A.

Proof. If HLP″ holds and $f \in X(C)$, then f^*, the decreasing rearrangement of $|f|$, also belongs to $X(C)$, and hence $\tilde{f}^* = \theta(f^*) \in X(C)$. By [2], pages 420-421, $\theta^*(x;f) \prec 2\theta(x;f^*)$. (This means that

$$\int_0^x \theta^*(t;f)\,dt \leqq 2\int_0^x \theta(t;f^*)\,dt$$

for all $x \geqq 0$.) Therefore

$$\int_0^1 c\theta\,dx \leqq \int_0^1 c^*\theta^*\,dx \leqq 2\int_0^1 c^*(x)\theta(x;f^*)\,dx \leqq 2\,\|\theta(f^*)\|,$$

so that $\theta(f) \in X(C)$, and we have established HLP. Also, if (6) is satisfied for all positive decreasing f, then (5) must hold. It will now be sufficient to show that HLP implies (6). Let $T_n f = \tilde{f}_n$ be the sequence of operators from $X(C)$ into itself, defined by placing $\tilde{f}_n(x) = \tilde{f}(x)$ or $\tilde{f}_n(x) = 0$ according as $1/n \leqq x \leqq 1$ or $0 \leqq x < 1/n$. By [3], Theorem 3.8.3, T_n are bounded linear operators. For $x > 1/n$ we have $-\theta(x;-f) \leqq \tilde{f}_n(x) \leqq \theta(x;f)$, hence there is a function F in $X(C)$, e.g., $F = |\theta(f)| + |\theta(-f)|$, so that $|\tilde{f}_n(x)| \leqq F(x)$ for all x and n. Also, $\tilde{f}_n(x) \to \tilde{f}(x)$ as $n \to \infty$. This implies that $\tilde{f}_n \to \tilde{f}$ in the norm of the space $X(C)$. Since the limit of a convergent sequence of linear bounded operators is bounded, we see that the operator $Tf = \tilde{f}$ has a bound. This establishes (6) and completes the proof.

For $f \in X(C)$, $f \geqq 0$ we have, with the notation (3),

$$(7) \qquad \begin{aligned} \|f\|_X &= \sup_{c \in C} \int_0^1 c(x)\,dx/x \int_0^x f(t)\,dt \\ &= \sup_{c \in C} \int_0^1 f(x)\,dx \int_x^1 c(t)/t\,dt = \sup_{c \in C} \int_0^1 f(x)\bar{c}(x)\,dx. \end{aligned}$$

The necessary and sufficient condition for $X(C) \in \mathrm{HLP}$ is, by the Lemma, that $\| \tilde{f} \| \leqq A \| f \|$, $f \in X(C)$. Remembering the definition of the dual space, we see that $X(C) \in \mathrm{HLP}$ is equivalent to $\| \bar{c} \|_{X'} \leqq A$. In this argument we could have restricted $f \in X(C)$ to be positive and decreasing. Let C^* denote the subclass of C consisting of all positive decreasing $c^* \in C$. Then instead of (7) we get, since $\tilde{f}(x)$ is positive and decreasing,

$$\| \tilde{f} \|_X = \sup_{c^* \in C^*} \int_0^1 c^*(x)dx/x \int_0^x f(t)dt = \sup_{c \in C^*} \int_0^1 f(x)\bar{c}(x)dx.$$

Hence we obtain:

THEOREM 1. *If C is rearrangement-invariant, then $X(C) \in \mathrm{HLP}$ if and only if for some constant A,*

$$\| \bar{c} \|_{X'} \leqq A \tag{8}$$

for all $c \in C$, or, equivalently, for all $c \in C^*$.

We note also another condition for $X(C) \in \mathrm{HLP}$. For $0 \leqq a \leqq 1$, let f_a denote the function $f_a(x) = f(ax)$. Since

$$\| \tilde{f} \| = \sup_{c \in C} \int_0^1 c(x)dx/x \left| \int_0^x f(t)dt \right| \leqq \sup_c \int_0^1 c(x)dx \int_0^1 |f(ax)|\, da$$

$$\leqq \int_0^1 \sup_c \int_0^1 |f(ax)|\, c(x)dx\, da = \int_0^1 \| f_a \|_X \, da,$$

we obtain by Lemma, that for $X(C) \in \mathrm{HLP}$ it is *sufficient* that for some constant A and all $f \in X(C)$,

$$\int_0^1 \| f_a \|_X \, da \leqq A \| f \|_X. \tag{9}$$

3. Spaces $\Lambda(\varphi)$ and $\mathbf{M}(\varphi)$. Let $\phi(x)$ be a decreasing positive integrable function on $(0,1)$, which we shall assume zero for $x > 1$, and let $\Phi(x) = \int_0^x \phi(t)dt$. The space $\Lambda(\phi)$ consists of all functions $f(x)$ such that

$$\| f \|_\Lambda = \int_0^1 \phi(x) f^*(x)dx = \sup_r \int_0^1 \phi_r(x) |f(x)|\, dx < +\infty ; \tag{10}$$

the supremum is taken over all rearrangements ϕ_r of ϕ. Dual with $\Lambda(\phi)$ is the space $\mathbf{M}(\phi)$ of functions f with

$$\| f \|_\mathbf{M} = \sup_a (1/\Phi(a)) \int_0^a f^*(t)dt < +\infty. \tag{11}$$

Obviously $\Lambda(\phi)$ and $\mathbf{M}(\phi)$ are spaces $X(C)$ with rearrangement-invariant C.

For $\Lambda(\phi)$, C^* consists of the single function ϕ. Applying Theorem 1 and formula (11) to this C^*, we see that $\Lambda(\phi) \varepsilon \mathrm{HLP}$ exactly if

$$\int_0^a dx \int_x^1 \phi(t)/t\, dt \leqq A \int_0^a \phi(t)\, dt, \qquad 0 \leqq a \leqq 1.$$

Changing the order of integrations we see that this is equivalent to the existence of a constant M such that

$$\int_a^1 \phi(x)/x\, dx \leqq Ma^{-1} \int_0^a \phi(x)\, dx, \qquad 0 \leqq a < 1. \tag{12}$$

This condition will be simplified.

THEOREM 2. *A space $\Lambda(\phi)$ has the Hardy-Littlewood property if and only if*

$$\limsup_{a \to 0} \Phi(2a)/\Phi(a) < 2. \tag{13}$$

Proof. If (13) holds, there is an a_0 and an $\epsilon > 0$ such that $\Phi(2a)/\Phi(a) < 2 - \epsilon$ for $0 < a \leqq a_0$. This quotient is a continuous function of a for $a \geqq a_0$, which can assume the value 2 only if $\phi(x)$ is constant, which is ruled out by (13). Hence we can assume that the inequality holds for all $0 < a \leqq 1$. Then we shall have

$$\int_a^{2a} \phi(x)\, dx \leqq (1-\epsilon) \int_0^a \phi(x)\, dx, \qquad 0 < a \leqq 1, \tag{14}$$

$$\int_0^{2^k a} \phi(x)\, dx \leqq 2^k (1-\epsilon/2)^k \int_0^a \phi(x)\, dx. \tag{15}$$

These two inequalities give

$$\begin{aligned}
\int_a^1 \phi(x)/x\, dx &\leqq \int_0^1 \phi(x)dx/(x+a) = \int_0^a + \int_a^{2a} + \cdots \\
&\qquad + \int_{2^{k-1}a}^{2^k a} \phi dx/(x+a) + \cdots \\
&\leqq 1/a \int_0^a \phi dx + (1-\epsilon)/a \int_0^a \phi dx + \cdots + (1-\epsilon)/(2^{k-1}a) \int_0^{2^{k-1}a} \phi dx + \cdots \\
&\leqq \{1 + (1-\epsilon) + (1-\epsilon)(1-\epsilon/2) + \cdots \\
&\qquad + (1-\epsilon)(1-\epsilon/2)^{k-1} + \cdots\} (1/a) \int_0^a \phi dx \\
&= (M/a) \int_0^a \phi dx,
\end{aligned}$$

with $M = (2-\epsilon)/\epsilon$. This proves that (13) is sufficient.

Now assume that (13) does not hold. We shall show that (12) is false for an arbitrarily large M.

For M chosen, take a natural number $n > 2M$ and an $\epsilon > 0$ so small that

$$\tfrac{1}{2}(1-2^n\epsilon)n > M. \tag{16}$$

By hypothesis, there is a b with $0 < b < 1$ such that

$$\int_0^{2b} \phi dx \geqq (2-\epsilon)\int_0^b \phi dx, \qquad \int_b^{2b} \phi dx \geqq (1-\epsilon)\int_0^b \phi dx. \tag{17}$$

Then

$$\int_{b/2}^{b} \phi dx \geqq (1-2\epsilon)\int_0^{b/2} \phi dx, \tag{18}$$

for otherwise we would have

$$\int_b^{2b} \phi dx \leqq 2\int_{b/2}^b < \int_{b/2}^b + (1-2\epsilon)\int_0^{b/2} \leqq (1-\epsilon)\int_0^b \phi dx,$$

which contradicts (17). Repeating this argument several times, we obtain for $k = 1, 2, \cdots, n$,

$$\int_{b/2^k}^{b/2^{k-1}} \phi dx \geqq (1-2^k\epsilon)\int_0^{b/2^k} \phi dx \geqq (1-\delta)\int_0^{b/2^k} \phi dx, \tag{19}$$

where $\delta = 2^n\epsilon$. Furthermore,

$$\int_0^{b/2^k} \phi(x)dx \geqq (2-\delta)\int_0^{b/2^{k+1}} \phi dx \geqq \cdots \geqq (2-\delta)^{n-k}\int_0^{b/2^n} \phi dx.$$

After these preparations we obtain for our special choice of b, by (18) and (19),

$$\begin{aligned}
\int_{b/2^n}^1 \phi(x)/x\,dx &\geqq 2^{n-1}/b\int_{b/2^n}^{b/2^{n-1}} \phi dx + 2^{n-2}/b\int_{b/2^{n-1}}^{b/2^{n-2}} + \cdots + 1/b\int_{b/2}^b \\
&\geqq (1-\delta)/b\{2^{n-1}\int_0^{b/2^n} + 2^{n-2}\int_0^{b/2^{n-1}} + \cdots + \int_0^{b/2}\} \\
&\geqq 2^{n-1}(1-\delta)/b\{\int_0^{b/2^n} + (1-\delta/2)\int_0^{b/2^n} + \cdots + (1-\delta/2)^{n-1}\int_0^{b/2^n}\} \\
&\geqq \tfrac{1}{2}(1-\delta)^n n\,2^n/b\int_0^{b/2^n} \phi dx.
\end{aligned}$$

Because of (16), we see that for the chosen M, (12) is violated for $a = b/2^n < 1$. Thus (13) is necessary.

THEOREM 3. *A space* $\mathbf{M}(\phi)$ *has the Hardy-Littlewood property if and only if, for some constant* A,

$$\int_0^a \Phi(x)/x\,dx \leqq A\Phi(a), \text{ for } 0 \leqq a \leqq 1, \tag{20}$$

Proof. The functions $c(x)$ of the class C^* are here $c(x) = \Phi(a)^{-1}$ or $c(x) = 0$ according as $0 \leqq x \leqq a$ or $a < x \leqq 1$. Since the dual to $\mathbf{M}(\phi)$ is $\Lambda(\phi)$, the condition (8) becomes

$$\int_0^1 \phi(x) \int_x^1 c(t)/t \, dt dx \leqq A,$$

and this is equivalent to (20).

4. Orlicz spaces. Let $0 \leqq \phi(u) \leqq +\infty$ be a function defined for $u \geqq 0$, increasing to infinity with u and vanishing for $u = 0$, but not identically 0 or $+\infty$ for all $u > 0$. Let $\psi(u)$ be its inverse, defined in a familiar way everywhere, except perhaps on a countable set of points corresponding to the discontinuities of ϕ. Let $\Phi(x)$ and $\Psi(x)$ be integrals of ϕ and ψ over $(0, x)$; Φ and Ψ are called conjugate functions (in sense of W. H. Young). The Orlicz space L_Φ consists of all functions $f(x)$ on $(0, 1)$ such that $\int_0^1 fg \, dx$ exists for all g with

$$I_\Psi(g) = \int_0^1 \Psi(|g|) dx < +\infty,$$

and we define

$$\| f \|_\Phi = \sup_{I_\Psi(g) \leqq 1} \int_0^1 fg \, dx.$$

This space L_Φ is a Banach space; it contains all functions f with $I_\Phi(f) < +\infty$, but in general also other functions. For example, if $\phi(u) = 0$ for $0 \leqq u \leqq 1$ and $\phi(u) = +\infty$ for $u > 1$, L_Φ is the space M of bounded functions, but $I_\Phi(f) < +\infty$ means that $|f(x)| \leqq 1$ a.e. However, L_Φ may be described as the set of all functions f such that for some $\lambda > 0$, $I_\Phi(\lambda f) < +\infty$; indeed, it may be shown [4] that $I_\Phi(f/\| f \|_\Phi) \leqq 1$. It follows that the spaces L_Φ, L_Ψ are dual to each other. Under the additional hypothesis that $\Phi(2u)/\Phi(u)$ is bounded, a stronger result is true: L_Ψ is the conjugate space to L_Φ. For the information of the reader we note that the boundedness of $\Phi(2u)/\Phi(u)$ is also necessary and sufficient for the space L_Φ to be separable. While the sufficiency of the condition is well known, its necessity seems to have escaped the attention of the writers on this subject until recently, when it was discovered independently by Mr. W. Luxemburg (Delft), Sobolev and Krasnosel'skiĭ, and the author.

THEOREM 4. *A space L_Φ has the Hardy-Littlewood property if and only if the conjugate function Ψ satisfies*

$$\Psi(2b) \leqq M\Psi(b), \qquad b \geqq b_0, \tag{21}$$

for some constants M and $b_0 > 0$.

Proof. It is easy to see that (21) implies the existence of two positive constants α, C such that

$$\Psi(ab) \leqq Ca^{\alpha}\Psi(b), \qquad b \geqq b_0, a > 1. \tag{22}$$

To prove that the condition is sufficient we shall show that it implies (9). For $f_a(x) = f(ax)$, $f \in L_\Phi$ we have with $c(x) \geqq 0$,

$$\| f_a \|_\Phi = \sup_{I_\Psi(c) \leqq 1} \int_0^1 | f(ax) | \, c(x) \, dx.$$

We shall begin by replacing arbitrary positive functions $c(x)$ by others such that, for each x, either $c(x) \geqq b_0$ of $c(x) = 0$. To achieve this, assume that $c(x) \geqq 0$ and $I_\Psi(c) \leqq 1$, and decompose the interval $(0,1)$ into two sets E_1, E_2 defined by the inequalities $c(x) < b_0$, and $c(x) \geqq b_0$. Since

$$\int_{E_1} | f(ax) | \, dx \leqq \int_0^1 | f(x) | \, dx \leqq A \| f \|_\Phi$$

(the last inequality follows from the fact that a small constant $c(x) = \lambda > 0$ satisfies $I_\Psi(c) \leqq 1$), we have

$$\| f_a \|_\Phi \leqq A \| f \|_\Phi + \sup_{I_\Psi(c') \leqq 1} \int_0^1 | f(ax) | \, c'(x) \, dx,$$

where the $c'(x)$ are such that either $c'(x) \geqq b_0$, or $c'(x) = 0$. On substitution $ax = t$ we obtain that the last supremum is

$$\sup_{\int_0^a \Psi(c')dt \leqq a} 1/a \int_0^a | f(t) | \, c'(t) \, dt \leqq \sup_{I_\Psi(c') \leqq a} 1/a \int_0^a | f(t) | \, c'(t) \, dt. \tag{23}$$

Assume first that $Ca \leqq 1$. Because of (22), $I_\Psi(c') \leqq a$ implies $I_\Psi((Ca)^{-1/\alpha}c') \leqq 1$. Applying this to (23) and replacing $(Ca)^{-1/\alpha}c'(t)$ by $c(t)$, we obtain in this case

$$\| f_a \|_\Phi \leqq A \| f \|_\Phi + \sup_{I_\Psi(c) \leqq 1} 1/a(Ca)^{1/\alpha} \int_0^1 | f | c dt = (C_1 a^{(1-\alpha)/\alpha} + A) \| f \|_\Phi.$$

For $Ca \geqq 1$, (23) readily gives $\| f_a \| \leqq C_2 \| f \|_\Phi$, and we obtain the condition (9).

We shall prove the necessity of (21) by means of Theorem 1. Assume that (21) does not hold. Taking into account the properties of Orlicz spaces, it will be sufficient to show that there is a function $c(x) \geqq 0$ which belongs

to L_Ψ and such that $I_\Psi(\lambda\tilde{c}) = +\infty$ for each $\lambda > 0$; this will imply that $\tilde{c} \notin L_\Psi$. If (21) does not hold and $\Psi(u)$ is finite for all $0 \leqq u < +\infty$, there must exist a sequence $b_k \to \infty$ such that $\Psi(2b_k)/\Psi(b_k) \to \infty$. Let the integers n_k be defined by

$$2^{-k-1} < 2^{-n_k}\Psi(b_k) \leqq 2^{-k}, \qquad k = 1, 2, \cdots. \tag{24}$$

We may assume (passing, if necessary, to a subsequence of the b_k) that $n_{k+1} > n_k + k$ and that $\Psi(2b_k)/\Psi(b_k) \geqq 2^{2k+1}$, so that

$$2^{-n_k}\Psi(2b_k) \geqq 2^k. \tag{25}$$

Now we define $c(x) = b_k$ for $2^{-n_k-k} \leqq x < 2^{-n_k}$, $k = 1, 2, \cdots$, and $c(x) = 0$ elsewhere. Then, by (24),

$$\int_0^1 \Psi(c)\,dx \leqq \sum 2^{-n_k}\Psi(b_k) \leqq \sum 2^{-k} < +\infty,$$

and therefore $c \in L_\Psi$. On the other hand, for each $\lambda > 0$ we have by definition of $\tilde{c}$,

$$\int_0^1 \Psi(\lambda\tilde{c})\,dx \geqq \sum_{k=1}^{\infty} \int_{2^{-n_k-k}}^{2^{-n_k-k+1}} \Psi\Big(\lambda \int_{2^{-n_k-k+1}}^{2^{-n_k}} b_k/t\,dt\Big)\,dx$$

$$= \sum_{k=1}^{\infty} 2^{-n_k-k}\Psi(\lambda b_k(k-1)\log 2).$$

For all sufficiently large values of k, say for $k \geqq k_0 = k_0(\lambda)$, the argument of Ψ in the last sum is greater than $2b_k$, and by (25), the series diverges. Hence $\int_0^1 \Psi(\lambda\tilde{c})\,dx = +\infty$.

In the case when (21) is violated in such a way that $\Psi(u)$ becomes infinite for finite u, the proof is similar, but somewhat simpler.

WAYNE UNIVERSITY.

REFERENCES.

[1] P. L. Butzer, "On Bernstein Polynomials," Thesis, University of Toronto (1951).

[2] G. G. Lorentz, "On the theory of spaces Λ," *Pacific Journal of Mathematics*, vol. 1 (1951), pp. 411-429.

[3] ———, *Bernstein Polynomials*, Toronto, 1953.

[4] A. C. Zaanen, *Linear Analysis*, New York and Amsterdam, 1953.

[5] A. Zygmund, *Trigonometric Series*, Warszawa-Lwów, 1935.

[6] H. W. Ellis and I. Halperin, "Function spaces," *Canadian Journal of Mathematics*, vol. 5 (1953), pp. 576-592.

ON ALGEBRAIC GROUPS AND HOMOGENEOUS SPACES*

By André Weil.

In a recent paper in the same Journal ([4] of the bibliography; quoted hereafter as AG), I gave some results on algebraic groups and transformation-spaces, which supplement those in my *Variétés abéliennes* ([3]; quoted as VA). Applications will now be made of that theory to somewhat more specific questions. In no. 1, a rather general procedure is described for obtaining, from a given transformation-space S with respect to a group G and from a suitable cycle on S, another transformation-space with respect to the same group. As shown in no. 2, this includes as a special case the construction of coset-spaces and of factor-groups; thanks to the main theorem in AG, these can now be defined without enlarging the groundfield, whereas such an enlargement was required in their construction as previously given by S. Nakano ([2]); except for this, we have substantially followed his method.

The rest of this paper is chiefly devoted to "principal homogeneous spaces," i.e. to those homogeneous spaces on which the group operates in a simply transitive manner. The pair consisting of such a space and of one point on it does not differ materially from a group; thus there is little incentive for studying those spaces as long as one is not paying any attention to the groundfield or if the groundfield is algebraically closed. But it can happen that a principal homogeneous space contains no rational point over the groundfield over which it is defined; an example of this is given by the plane curve $X^3 + pY^3 = p^2$ over the rational number-field, where p is a rational prime; this may be considered as a principal homogeneous space with respect to its jacobian variety, which is the plane curve $Y^2 = 4X^3 - 27$. More generally, Chow's work (cf. [1]) has shown that it is not always possible to map a curve "canonically" into its jacobian variety by a mapping defined over the groundfield, but that the curve can always be so mapped into a suitable principal homogeneous space with respect to its jacobian variety. This, among other results, will be proved again here by a different method, which can be extended at once to a variety V of higher dimension and to its Albanese variety, provided the groundfield is one over which the latter is defined. It will also be shown that the classes of principal homogeneous

* Received December 27, 1954.

spaces with respect to a commutative group can be arranged into a torsion-group, i.e. a group whose elements are all of finite order; and it follows at once from the results of no. 5 that this group must be countable if the groundfield is finitely generated over the prime field. There seems to be no reason why it should be finite, even if the groundfield is the field of rational numbers; a more detailed investigation of its structure, e.g. for the case of an elliptic curve over the field of rational numbers, would be of considerable interest from the point of view of the theory of diophantine equations.

1. Let G be a group and S a transformation-space with respect to G, both defined over a field k. Let Z be either a divisor on S or a cycle on S whose components have coefficients which are prime to the characteristic of the universal domain. We denote by sZ, for any $s \in G$, the transform of Z by the mapping $u \to su$ of S onto itself. Let K be an overfield of k over which Z is rational. Let x be generic over K on G; by Prop. 6 of the Appendix of AG, there is a finitely generated extension $k(t)$ of k which is the smallest overfield of k over which xZ is rational; as xZ is rational over $K(x)$, we have $k(t) \subset K(x)$. If x' is also a generic point of G over K, and σ is the isomorphism of $K(x)$ onto $K(x')$ over K which maps x onto x', σ will transform xZ into $x'Z$; if t' is the image of t under σ, $k(t')$ will then be the smallest overfield of k over which $x'Z$ is rational, and, by Prop. 6 of the Appendix of AG, the cycle $x'Z$ depends only upon t'; in other words, if σ_1 is an isomorphism of $K(x)$ onto a field $K(x_1')$, mapping x onto x_1' and t onto t_1', we have $x'Z = x_1'Z$ if and only if $t' = t_1'$. In particular, take $x' = yx$, with y generic over $K(x)$ on G; then $k(t')$ is the smallest overfield of k over which yxZ is rational; as yxZ can be written as $y(xZ)$, it is rational over $k(y,t)$, so that $k(t') \subset k(y,t)$; similarly, xZ can be written as $y^{-1}(yxZ)$ and is therefore rational over $k(y,t')$, so that $k(t) \subset k(y,t')$. This shows that $k(y,t) = k(y,t')$.

Put now $z = yx$, so that we have $k(t') \subset K(z)$; take y' generic over $K(x,y)$ on G, and call τ the isomorphism of $K(z)$ onto $K(y'z)$ over K which maps z onto $y'z = y'yx$; let t'' be the image of t' under τ. Then t'' is the image of t under the isomorphism $\tau \circ \sigma$ of $K(x)$ onto $K(y'yx)$ over K which maps x onto $y'yx$.

If Z is such that $k(t)$ is a regular extension of k, then we may call T the locus of t over k and, with the above notations, we may write $t' = g(y,t)$, where g is a mapping of $G \times T$ into T, defined over k. Then the results we have just proved mean that g satisfies (TG 1, 2) of AG, no. 2, i.e. that it is a normal law between G and T. Applying now the main theorem of AG, we get the following result:

PROPOSITION 1. *Let G be a group and S a transformation-space with respect to G, both defined over a field k. Let Z be either a divisor on S or a cycle on S whose components have coefficients which are prime to the characteristic. Let K be an overfield of k over which Z is rational; and assume that, if x is generic over K on G, the smallest extension k' of k over which xZ is rational is a regular extension of k. Then there is a transformation-space T with respect to G, defined over k, and an everywhere defined mapping F of G into T, defined over K, such that the point $t = F(x)$ is generic over k on T, that $k' = k(t)$, and that $F(ss') = sF(s')$ for all s, s' on G. For any s, s' in G, we have $F(s) = F(s')$ if and only if $sZ = s'Z$. If Z is algebraic over k, one can take for T a homogeneous space with respect to G.*

The existence of a transformation-space T with a generic point t over k such that $k' = k(t)$ has been proved above; moreover, with the same notations as above, we have $k(t) \subset K(x)$, $k(t') \subset K(yx)$, $t' = yt$; as $K(x)$, $K(yx)$ are independent extensions of K, this shows, if K is algebraic over k, that $k(t)$, $k(t')$ are then independent extensions of k, i.e. that T is pre-homogeneous, so that, by the main theorem of AG, we may replace it by a birationally equivalent homogeneous space. As $k(t) \subset K(x)$, we may write $t = F(x)$, with F defined over K; then we have $yt = F(yx)$, i.e. $F(yx) = yF(x)$, for y generic over $K(x)$ on G. This may be written as $F(x) = y^{-1}F(yx)$, which shows, if s is any point of G and y is taken generic over $K(s)$ on G, that F is defined at s. As F is everywhere defined, the relation $F(yx) = yF(x)$ implies $F(ss') = sF(s')$ for all s, s' on G. Now, for any s, s' on G, take x generic over $K(s, s')$ on G; then xs, xs' are both generic over K on G, and therefore, if σ is the isomorphism of $K(xs)$ onto $K(xs')$ over K which maps xs onto xs', σ will map $F(xs)$ onto $F(xs')$ and the cycle xsZ onto $xs'Z$; then, as we have seen above, we have $xsZ = xs'Z$ if and only if $F(xs) = F(xs')$; as the latter relation can be written $xF(s) = xF(s')$, so that these two relations are respectively equivalent to $sZ = s'Z$ and to $F(s) = F(s')$, this completes our proof.

2. We first apply Prop. 1 to the construction of the homogeneous space defined by a group G and a subgroup of G.

PROPOSITION 2. *Let G be a group, defined over a field k; let Z be a rational cycle over k on G, consisting of components with coefficient* 1, *and such that its support $|Z|$ is a subgroup of G. Then there is a homogeneous space H with respect to G, defined over k, and a rational point a over k on H, with the following properties*: (i) *if we put, for a generic x over k on G,*

$F(x) = xa$, the mapping F of G onto H determines a one-to-one mapping of the cosets of $|Z|$ in G onto the points of H; (ii) *$k(x)$ is separable over $k(F(x))$;* (iii) *if ϕ is a mapping of G into a variety V, defined over an overfield K of k, and such that $\phi(xs) = \phi(x)$ whenever $s \in |Z|$ and x is generic over $K(s)$ on G, there is a mapping ψ of H into V, defined over K, such that $\phi = \psi \circ F$. If $|Z|$ is a normal subgroup of G, then one can define on H a group-law, defined over k, such that F is a homomorphism of G onto H.*

The "support" of a cycle was defined at the beginning of the Appendix of AG. The assumption on $|Z|$ implies that Z has one and only one component Z_0 containing e, that this is a subgroup of G, and that all the components of Z are cosets of Z_0 in G. We apply Prop. 1 to the cycle Z on $S = G$, G acting on itself by the left-translations, and to the field k; if x is generic over k on G, the smallest extension of k over which xZ is rational is contained in $k(x)$, and hence, by AG-App., Prop. 3, Coroll., it is regular over k. Therefore, by Prop. 1, there is a homogeneous space with respect to G, which we now call H, defined over k, and a mapping F of G into H, defined over k, with the properties stated in Prop. 1; in particular, F is everywhere defined, $t = F(x)$ is generic over k on H, and $k(t)$ is the smallest extension of k over which xZ is rational. If we put $a = F(e)$, a is rational over k, and we have, for all $s \in G$, $F(s) = sa$. If s, s' are any two points on G, we have $sa = s'a$ if and only if $sZ = s'Z$, i.e. if and only if $s^{-1}s'Z = Z$; by the assumption on Z, the latter relation is equivalent to $s^{-1}s' \in |Z|$. Thus the points of H are in a one-to-one correspondence with the cosets of $|Z|$ in G.

Call Γ the graph of F on $G \times H$. For any $b \in H$, $\Gamma \cap (G \times b)$ is the set of those points (s, b) which are such that $sa = b$; in particular, if x is generic over k on G and if we put $t = F(x) = xa$, $\Gamma \cap (G \times t)$ is the set of the points (s, t) such that $sa = xa$, i.e. $x^{-1}s \in |Z|$; this set can be written as $|xZ| \times t$. As $\Gamma \cdot (G \times t)$ is the prime rational cycle over $k(t)$ on $G \times H$ with the generic point (x, t) over $k(t)$, this shows that the prime rational cycle Z' over $k(t)$ on G with the generic point x has the same components as the cycle xZ; as the latter is rational over $k(t)$ and its components have the coefficient 1, this implies that $Z' = xZ$. As the components of the prime rational cycle with the generic point x over $k(t)$ have the coefficient 1, $k(x)$ must be separable (i.e. "separably generated") over $k(t)$.

As to (iii), let x be generic over K on G; put $t = F(x)$ and $w = \phi(x)$; let w' be any generic specialization of w over $K(t)$; this can be extended to a generic specialization x' of x over $K(t)$; we have then $w' = \phi(x')$

and $t = F(x')$, and the latter relation implies that x' is on $|xZ|$, i.e. that it is of the form xs with $s \in |Z|$. Let $\bar{x}$ be generic on G over $K(s)$; we have $\phi(\bar{x}s) = \phi(\bar{x})$; specializing $\bar{x}$ to x over $K(s)$, we get $\phi(xs) = \phi(x)$, since both sides are defined, i.e. $w' = w$. This shows that w is purely inseparable over $K(t)$; as it is at the same time rational over $K(x)$ which is separable over $K(t)$, it is therefore rational over $K(t)$, and we may write $w = \psi(t)$, where ψ is a mapping of H into V, defined over K. This proves (iii).

Finally, assume that $|Z|$ is a normal subgroup of G; let x, y be independent generic points of G over k; put $t = F(x)$, $u = F(y)$. We have $F(xy) = xF(y) = xu$; this is a function of x, defined over $k(u)$. If $s \in |Z|$, we have $xsy = xys'$ with $s' = y^{-1}sy \in |Z|$, and therefore $F(xsy) = F(xy)$; by (iii) applied to the mapping $x \to xu$ of G into H and to $K = k(u)$, this implies that $F(xy)$ is rational over $k(u,t)$. Therefore the mapping $u \to xu$ of H into H is defined over $k(t)$; on the other hand, if k' is any field of definition for that mapping, containing k, the image $xa = t$ of a by it is rational over k', so that $k(t) \subset k'$; thus $k(t)$ is the smallest field of definition for the mapping $u \to xu$. This shows that G is not operating faithfully on H; applying Prop. 2 of AG, no. 3, to G and H, we see that we can define on H a normal law of composition f such that $F(xy) = f(F(x), F(y))$. By the main theorem of AG, we can then replace H by a birationally equivalent group H', defined over k, with a mapping F' of G into H', also defined over k, such that $F'(xy) = F'(x)F'(y)$, $F(x)$ and $F'(x)$ being corresponding generic points of H and H' over k when x is generic over k on G. As usual, from the relation $F'(x) = F'(y)^{-1}F'(yx)$ which holds for x, y generic and independent over k, we deduce that F' is everywhere defined[1]; therefore, if G is made to operate on H' by the law $(x, w) \to F'(x)w$ for x, w generic and independent over k on G and H', H' is a homogeneous space with respect to G. But then the unicity assertion in the main theorem of AG can be applied to H and H' and shows that they are biregularly equivalent; in other words, H itself, with the law f, is a group. This completes the proof.

It is easily seen that the pair (H, a) is uniquely determined, up to an isomorphism, by the conditions (i), (ii), (iii) in Prop. 2; in other words, if H' and a' have similar properties, there is an everywhere biregular birational correspondence between H and H' which maps a onto a' and transforms the law of composition between G and H into the law between G and H'. The space H may be called the *coset-space* determined by G and Z, and may be denoted by G/Z; if $|Z|$ is a normal subgroup of G, the space H, with the group-law

[1] This is Theorem 1 of Nakano ([2]).

determined by Prop. 2, is called the *quotient-group* (or factor-group) of G by Z, and is denoted by G/Z.

3. Before making another application of Prop. 1, we will introduce a new condition which a law of composition may satisfy. Let V, W be two varieties, g a mapping of $V \times W$ into W, and k a field of definition for V, W and g; consider the following condition:

(TG 1′) *If x, u are independent generic points of V, W over k, and $v = g(x, u)$, then $k(x, u) = k(x, v) = k(u, v)$.*

The condition $k(x, u) = k(x, v)$ is equivalent to (TG 1) of AG, no. 2. The condition $k(x, u) = k(u, v)$ implies that the dimension of V, which is the dimension of x over $k(u)$, is the same as that of v over $k(u)$, and therefore at most that of W; if the dimensions of V and of W are the same, this implies that v is generic over $k(u)$ on W, which is condition (H) of AG, no. 2. Let k' be any field of definition containing k for the birational correspondence $u \to v = g(x, u)$ between W and itself; if u is taken generic over $k'(x)$ on W, we have $k'(u) = k'(v)$; since $k(x) \subset k'(u, v)$ by (TG 1′), we have $k(x) \subset k'(u)$. Taking u' generic on W over $k'(x, u)$, we get in the same manner $k(x) \subset k'(u')$. As $k'(u)$, $k'(u')$ are independent regular extensions of k', their intersection is k', so that $k(x) \subset k'$. This shows that (TG 1′) implies (TG 3). In view of the results of AG, end of no. 3, this shows that, if g satisfies (TG 1′) and (TG 2′), or if two mappings f, g of $V \times V$ into V and of $V \times W$ into W are given and satisfy (TG 1′. 2), then V is a pre-group and W a pre-transformation space, and V operates faithfully on W.

If a pre-group V and a pre-transformation space W satisfy (TG 1′), we say that W is a *pre-principal space* with respect to V; if at the same time V and W have the same dimension, so that, as we have shown, W is prehomogeneous with respect to V, we also say that V is *simply pre-transitive on W*.

Let W be a pre-principal space with respect to a pre-group V; by the main theorem of AG, we can construct a group G and a transformation-space S, birationally equivalent to V, W and defined over the same field k; then S is also pre-principal with respect to G. Let T be the locus of (u, xu) over k on $S \times S$, x and u being independent generic points of G, S over k; put $t = (u, xu)$; then (TG 1′) implies that $k(x) \subset k(t)$, i.e. that we may write $x = \phi(t)$, where ϕ is a mapping of T into G, defined over k; conversely, if this is so for a transformation-space S with respect to G, S is pre-principal.

The space S will be called a *principal space with respect to* G if, for x, u generic and independent over k on G, S and for $t = (u, xu)$, we have $x = \phi(t)$ where ϕ is an *everywhere defined mapping*, defined over k, of the locus T of t over k into the group G. If at the same time S is homogeneous, it will be called a *principal homogeneous space* with respect to G.

PROPOSITION 3. *Let S be a pre-principal transformation-space with respect to a group G, both being defined over a field k. Then there is a k-open subset P of S which is a principal transformation-space with respect to G; if G and S have the same dimension, P is uniquely determined and is homogeneous.*

Let T and ϕ be defined as above; call F the k-closed subset of T where ϕ is not defined. We first show that, if (a, b) is in F, $(sa, s'b)$ is in F for all s, s' in G. In fact, take x, u generic and independent over $k(s, s')$ on G, S; put $v = xu$, $u_1 = su$, $v_1 = s'v$, $x_1 = s'xs^{-1}$; then we have $v_1 = x_1u_1$, and x_1, u_1 are generic and independent over $k(s, s')$ on G, S, so that (u, v) and (u_1, v_1) are generic points of T over $k(s, s')$, and that $x = \phi(u, v)$, $x_1 = \phi(u_1, v_1)$ by the definition of ϕ; this gives

$$\phi(u, v) = s'^{-1}\phi(su, s'v)s.$$

If (a, b) is in T, it is a specialization of (u, v) over $k(s, s')$, and therefore $(sa, s'b)$ is also in T; then the above relation shows that ϕ is defined at (a, b) if it is defined at $(sa, s'b)$, i.e. that $(a, b) \in F$ implies $(sa, s'b) \in F$.

As (e, u) is a specialization of (x, u) over k, e being the neutral element of G, T contains the diagonal Δ of $S \times S$. As the projection of Δ on either factor of $S \times S$ is everywhere biregular, the projection of the k-closed subset $F \cap \Delta$ of Δ onto S is a k-closed subset F' of S, consisting of the points $a \in S$ such that ϕ is not defined at (a, a). From what we have proved above, it follows that, if $a \in F'$, $sa \in F'$ for all $s \in G$. For the same reason, if a is in $S - F'$, then $\phi(a, sa)$ is defined for all $s \in G$; as (a, sa, s) is then a specialization of (u, xu, x) over k, and $x = \phi(u, xu)$, this shows that $\phi(a, sa) = s$ for all $a \in S - F'$ and all $s \in G$, and therefore $k(a, s) = k(a, sa)$; in particular, if x is generic over $k(a)$ on G, the locus of xa over $k(a)$ has a dimension equal to that of G.

If G is complete, every specialization (a, b) of (u, xu) over k can be extended to a specialization (a, b, s) of (u, xu, x) over k, so that $b = sa$; in other words, every point of T must be of the form (a, sa), with $a \in S$ and $s \in G$; then it follows from what we have proved above that such a point cannot be in F unless a and sa are in F'. Without attempting to decide whether this is still so in the general case, we shall merely show that, if u

is generic over k on S and (u, u') is in F, then u' must be in F'. In fact, suppose that this is not so; take x generic over $k(u, u')$ on G; call X, X' the loci of xu, xu' over $k(u, u')$ on S; by what we have proved above, they have the same dimension, which is that of G. By F-VI$_3$, Th. 11, we have $T \cap (u \times S) = u \times X$; at the same time, since we have shown that (u, xu') is in T, $u \times X'$ is contained in $T \cap (u \times S)$; as X and X' have the same dimension, this implies that $X = X'$. But, as we have shown, since (u, u') is in F, (u, xu') must be in F, and therefore, since F is k-closed, $u \times X'$ must be contained in F; as $X = X'$, this implies that F contains (u, xu), which is generic on T over k, and contradicts the definition of F. One may observe that, if S is pre-homogeneous, this again shows that (a, b) cannot be in F unless a, b are in F'; for, if $a \notin F'$ and x is generic on G over $k(a, b)$, xa has then over $k(a)$ a dimension equal to that of G, and therefore is generic on S over $k(a)$ since in the present case the dimensions of S and G are equal; then if (a, b) is in F, so is (xa, b), and so b must be in F'.

Now replace first S by $S - F'$; as F' is mapped onto itself by all operations of G, $S - F'$ is again a transformation-space with respect to G, defined over k, and satisfies our other assumptions. Writing again S instead of $S - F'$, we see that it is enough to prove our result under the additional assumption that $F' = \emptyset$. If G is complete or S is prehomogeneous, this already implies that S is principal. Otherwise we observe that, since T is also the locus of $(x^{-1}u, u)$ over k and since we have $\phi(x^{-1}u, u) = x$, T and F are mapped onto themselves by the mapping $(u, v) \to (v, u)$ of $S \times S$ onto itself. Call now F'' the "projection" of F on either factor of $S \times S$ (in the sense of F-IV$_3$ and F-VII$_3$, i.e. the closure of the set-theoretic projection); this will be the same, whether we project F onto the first or the second factor, and it is not S by what we have proved above, since F' is empty; it is therefore a k-closed subset of S. By what we have proved, F'' is mapped onto itself by all operations of G. Then $S - F''$ is the principal space whose existence was to be proved.

Finally, assume that the space S from which we first started was pre-homogeneous; this means that $T = S \times S$. Let a, b be any two points in $S - F'$; then, if x is generic on G over $k(a, b)$, xa, xb are generic on S over $k(a, b)$, and so there is an isomorphism σ of $k(a, b, xa)$ onto $k(a, b, xb)$ over $k(a, b)$, mapping xa onto xb; then we have $x^\sigma a = xb$, i.e. $b = x^{-1}x^\sigma a$. This shows that $S - F'$ is homogeneous, and also that an open subset of S which is a transformation-space for G cannot contain a point of $S - F'$ without containing $S - F'$. Therefore $S - F'$ is the only open subset of S which is a principal space with respect to G.

If S is a principal homogeneous space, the mapping ϕ of $T = S \times S$ into G which has been defined above will be called the *canonical mapping* of $S \times S$ into G. For any a, b on S and s on G, the relations $b = sa$, $s = \phi(a, b)$ are equivalent; in particular, for any a on S and for x generic over $k(a)$ on G, the mapping $x \to xa = v$ of G into S has the inverse $v \to x = \phi(a, v)$; as both are everywhere defined, this is therefore an everywhere biregular mapping of G onto S, defined over $k(a)$. In particular, if there is at least one rational point a over k on S, S is biregularly equivalent to G over k.

4. Let G be a group, V and W two varieties, and F a mapping of $V \times W$ into G, all defined over a field k. We may consider $W \times G$ as a transformation-space with respect to G, the law of composition between them being $(x, (N, y)) \to (N, xy)$ for any N in W and any x, y in G. We now apply Prop. 1 of no. 1 to the case when we take for S this transformation-space $W \times G$ and for Z the graph of the mapping $N \to F(M, N)$ of W into G, where M, N are independent generic points of V, W over k. We must then consider the smallest field of definition k' containing k for the mapping $N \to xF(M, N)$ of W into G, where x is generic over $k(M, N)$ on G. As this mapping is defined over $k(x, M)$, k' is a regular extension of k, contained in $k(x, M)$. Then Prop. 1 shows that we may write $k' = k(u)$, where u is a generic point over k of a transformation-space U with respect to G; as $k(u) \subset k(x, M)$, we may write $u = f(x, M)$, where f is a mapping of $G \times V$ into U, defined over k; moreover, as the mapping $x \to f(x, M)$ of G into U is no other than the mapping F defined in Prop. 1, we see that f is defined at every point (s, M) of $G \times M$, and that $f(ss', M) = sf(s', M)$; taking $s' = e$, and writing $f(M)$ instead of $f(e, M)$, this gives $f(s, M) = sf(M)$, and in particular $u = xf(M)$. As the mapping $N \to xF(M, N)$ is defined over $k(u)$, $xF(M, N)$ is rational over $k(u, N)$; similarly, if y is generic over $k(x, M, N)$ on G, the mapping $N \to yxF(M, N)$ is defined over $k(yu)$, and so $yxF(M, N)$ is rational over $k(yu, N)$. As we can write

$$y = (yxF(M, N))\,(xF(M, N))^{-1},$$

this shows that y is rational over $k(u, yu, N)$. If N' is generic on W over $k(x, y, M, N)$, y must then also be rational over $k(u, yu, N')$; thus $k(y)$ is contained in $k(u, yu, N)$ and in $k(u, yu, N')$; as these are independent regular extensions of $k(u, yu)$, their intersection is $k(u, yu)$, and so we have $k(y) \subset k(u, yu)$. This means that U is a pre-principal space and may therefore, by Prop. 3, be replaced by a principal space, birationally equivalent to it.

The most interesting case is that in which there are two mappings F_1, F_2 of V, W into G, defined over some overfield K of k, such that $F(M,N) = F_1(M)F_2(N)$ for M, N generic and independent over K on V, W; by the corollary of Th. 7, VA-18, this is always so whenever G is an abelian variety. Take x generic over $K(M,N)$ on G, and put $z = xF_1(M)$; then the mapping $N \to xF(M,N) = zF_2(N)$ is defined over $K(z)$, so that $k(u) \subset K(z)$. As x, M are generic and independent over $K(N)$ on G, V, u is then generic over $K(N)$ on U, and the dimension of U is that of u over K; the relation $K(u) \subset K(z)$ shows that this is at most the dimension of G. Therefore U is pre-homogeneous and may be taken to be a principal homogeneous space with respect to G. Moreover, we may write $u = \Phi(z)$, where Φ is a mapping of G into U, defined over K. If we substitute yx for x, with y generic over $K(M,N,x)$ on G, z is replaced by yz, and u by yu; this gives $\Phi(yz) = y\Phi(z)$, which may be written as $\Phi(z) = y^{-1}\Phi(yz)$ and thus shows that Φ is everywhere defined. Putting now $a = \Phi(e)$, we see that a is rational over K and that $u = za$, i.e. $f(M) = F_1(M)a$. Put now $g(N) = F_2(N)^{-1}a$; g is a mapping of W into U, defined over K. As we have also $g(N) = F(M,N)^{-1}f(M)$, g is also defined over the field $k(M)$, and therefore also over $k(M')$ if M' is another generic point of V over K; if we take M, M' generic and independent over K on V, $k(M)$ and $k(M')$ are independent regular extensions of k, so that their intersection is k; hence g is defined over k. Thus we have proved the following result:

PROPOSITION 4. *Let G be a group, V and W two varieties and F a mapping of $V \times W$ into G, all defined over k. Assume that there are two mappings F_1, F_2 of V, W into G, defined over some overfield K of k, such that $F(M,N) = F_1(M)F_2(N)$ for M, N generic and independent over K on V, W. Then there is a principal homogeneous space U with respect to G, and two mappings f, g of V, W into U, all defined over k, such that $f(M) = F(M,N)g(N)$, i.e. $F(M,N) = \phi(g(N), f(M))$, where ϕ is the canonical mapping of $U \times U$ into G.*

COROLLARY. *Notations being as in Prop. 4, U, f and g are uniquely determined by G, V, W and F, up to an isomorphism.*

In fact, assume that U', f', g' have similar properties; then we have $xF(M,N) = \phi'(g'(N), xf'(M))$, where ϕ' is the canonical mapping for U'. This shows that the mapping $N \to xF(M,N)$ is defined over $k(u')$ with $u' = xf'(M)$; thus, if we put $u = xf(M)$ as before, we have $k(u) \subset k(u')$ and may write $u = \psi(u')$, where ψ is a mapping of U' into U, defined over k.

Replacing x by yx, with y generic on G over $k(M,N,x)$, we get $yu=\psi(yu')$; from this we conclude, in the usual manner, that ψ is everywhere defined. Take any point a' on U', and put $a=\psi(a')$; as we have $xa=\psi(xa')$, and as the mappings $x\to xa$, $x\to xa'$ are everywhere biregular mappings of G onto U and U', defined over $k(a')$, we see that ψ is an everywhere biregular mapping of U' onto U. Moreover, we have $\psi(u')=x\psi(f'(M))$, and therefore $f=\psi\circ f'$; from this one easily concludes that $g=\psi\circ g'$. This proves our assertion.

5. Let G be a group, defined over a field k. We will now prove that the classes of principal homogeneous spaces with respect to G, for birational equivalence over k, form a set. In fact, let x, y be independent generic points of G over k; let σ be the isomorphism of $\bar{k}(x)$ onto $\bar{k}(yx)$ over $\bar{k}$ which maps x onto yx. Let H be any principal homogeneous space with respect to G, defined over k; let a be an algebraic point over k on H, and put $u=xa$, so that u is generic over k on H. Then $k(u)$ is a regular extension of k contained in $\bar{k}(x)$ and such that $\bar{k}(u)=\bar{k}(x)$; moreover, we have

$$k(y,u)=k(y,u^\sigma)=k(u,u^\sigma)$$

since $u^\sigma=yu$. Conversely, let $k(u)$ be any such extension of k, and call U the locus of u over k; then we may write $u^\sigma=g(y,u)$, where g is a mapping of $G\times U$ into U, defined over k; and one verifies at once that this makes U into a pre-principal pre-homogeneous space with respect to G, and thus determines uniquely a class of birationally equivalent principal homogeneous spaces with respect to G. As every such class is determined by at least one such extension, this shows that these classes form a set.

If G is commutative, one can define canonically a commutative group-structure on the set of classes of principal homogeneous spaces with respect to G. In order to do this, we first observe that, if H is any transformation-space over a commutative group G, then the law $(x,u)\to x^{-1}u$, for $x\in G$, $u\in H$, defines on H a structure of transformation-space with respect to G; this will be called the *opposite* transformation-space to H and will be denoted by H^-; it is a principal homogeneous space if H is such.

PROPOSITION 5. *Let G be a commutative group, defined over a field k. Let H_i, for $1\leqq i\leqq n$, be principal homogeneous spaces with respect to G, defined over k. Then there is a principal homogeneous space H with respect to G, defined over k, and an everywhere defined mapping f of $H_1\times H_2\times\cdots\times H_n$ into H, defined over k, such that*

$$f(s_1a_1,\cdots,s_na_n)=s_1\cdots s_nf(a_1,\cdots,a_n)$$

for all $s_i \in G$ and $a_i \in H_i$. Moreover, H and f are uniquely determined up to an isomorphism of H.

Put $V = W = H_1 \times H_2 \times \cdots \times H_n$; call ϕ_i the canonical mapping of $H_i \times H_i$ into G, so that $b_i = sa_i$ is equivalent to $s = \phi_i(a_i, b_i)$ for a_i, b_i in H_i and s in G. Let $u = (u_1, \cdots, u_n)$ and $v = (v_1, \cdots, v_n)$ be two points of V; put

$$F(u, v) = \prod_{i=1}^{n} \phi_i(u_i, v_i),$$

where the right-hand side has a meaning since G is commutative. On each H_i, choose a point a_i, and put $a = (a_1, \cdots, a_n)$. We have

$$\phi_i(u_i, v_i) = \phi_i(a_i, v_i)\phi_i(a_i, u_i)^{-1}$$

for all i, as one verifies at once, and therefore, again because of the commutativity of G:

$$F(u, v) = F(a, v)F(a, u)^{-1}.$$

Thus the assumptions of Prop. 4 are satisfied, so that there is a principal homogeneous space U and two mappings f, g of V into U, all defined over k, such that

$$f(u) = F(u, v)g(v), \qquad F(u, v) = \phi(g(v), f(u)), \tag{1}$$

where ϕ is the canonical mapping of $U \times U$ into G. Take any point b on V, and take v generic over $k(b)$ on V; as F is defined at (b, v), the relation (1) shows that f is defined at b. Thus f is everywhere defined. As $F(u, u) = e$, the relation (1) gives $g(u) = f(u)$, i.e. $f = g$. If $s_1, \cdots, s_n$ are any elements of G, and we put $s = s_1 \cdots s_n$ and $u' = (s_1u_1, \cdots, s_nu_n)$, we have $F(u', v) = s^{-1}F(u, v)$ and therefore, by (1), $f(u') = s^{-1}f(u)$. If we now put $H = U^-$, i.e. if we take for H the opposite space to U, H and f will have the properties stated in Prop. 5.

Let us now assume that $\bar{H}$ and $\bar{f}$ have similar properties; put $\bar{U} = \bar{H}^-$. Put $\bar{z} = F(u, v)^{-1}\bar{f}(u)$, the multiplication in the right-hand side being that of $\bar{U}$. If the s_i, s and u' have the same meaning as above, we have $\bar{f}(u') = s^{-1}\bar{f}(u)$, so that $\bar{z}$ does not change if one replaces u, v by u', v. Therefore $k(\bar{z})$ is contained both in $k(u, v)$ and in $k(u', v)$. If the s_i have been taken generic and independent over $k(u, v)$ on G, $k(u, v)$ and $k(u', v)$ will be independent regular extensions of $k(v)$; this gives $k(\bar{z}) \subset k(v)$, so that we may write $\bar{z} = \bar{g}(v)$, with $\bar{g}$ defined over k. Then we have $\bar{f}(u) = F(u, v)\bar{g}(v)$; by the corollary of Prop. 4, $\bar{U}$, $\bar{f}$ and $\bar{g}$ must then be

the same as U, f and f, respectively, except for an isomorphism of U onto $\bar{U}$. This proves the assertion about unicity in Prop. 5.

In Prop. 5, take $n=2$; call $\mathfrak{H}_1$, $\mathfrak{H}_2$ the classes of H_1, H_2, and denote by $\mathfrak{H}_1+\mathfrak{H}_2$ the class of H. This defines on the set of classes of principal homogeneous spaces with respect to G a commutative group-structure. In fact, commutativity is obvious. Call $\mathfrak{H}_0$ the class of G, and therefore of all principal homogeneous spaces with respect to G which have a rational point over k. For any principal homogeneous space H with respect to G, the mapping $f(x,u)=xu$ of $G\times H$ into H satisfies the condition of Prop. 5; therefore we have $\mathfrak{H}_0+\mathfrak{H}=\mathfrak{H}$ for all classes $\mathfrak{H}$. If ϕ is the canonical mapping of $H\times H$ into G, then ϕ, considered as a mapping of $H\times H^-$ into G, satisfies the condition of Prop. 5; therefore, if $\mathfrak{H}^-$ is the class of H^-, we have $\mathfrak{H}+\mathfrak{H}^-=\mathfrak{H}_0$. Finally, let H_1, H_2, H_3 be three principal homogeneous spaces with respect to G; apply Prop. 5 successively to the following spaces: (a) to H_1, H_2, obtaining a space H_{12} and a mapping f_{12}; (b) to H_{12}, H_3, obtaining H', f'; (c) to H_2, H_3, obtaining H_{23}, f_{23}; (d) to H_1, H_{23}, obtaining H'', f''; (e) to H_1, H_2, H_3, obtaining H, f. Then the two mappings

$$f'(f_{12}(u_1,u_2),u_3), \qquad f''(u_1,f_{23}(u_2,u_3))$$

of $H_1\times H_2\times H_3$ into H', H'' satisfy the same condition as the mapping f. By the unicity assertion of Prop. 5, this shows that H', H'' are isomorphic to H. This means that the addition $\mathfrak{H}_1+\mathfrak{H}_2$ is associative.

One proves quite similarly, by induction on n, that if $\mathfrak{H}$ and $\mathfrak{H}_i$ are the classes of the spaces H, H_i in Prop. 5, then $\mathfrak{H}=\sum_i \mathfrak{H}_i$. In fact, let H', f' be the space and the mapping obtained by applying Prop. 5 to $H_1,\cdots,H_{n-1}$, so that $\mathfrak{H}'=\mathfrak{H}_1+\cdots+\mathfrak{H}_{n-1}$ by the induction assumption; and let H'', f'' be the space and the mapping obtained by applying Prop. 5 to H', H_n, so that $\mathfrak{H}''=\mathfrak{H}'+\mathfrak{H}_n$ by definition. Then the mapping

$$(u_1,\cdots,u_n)\to f''(f'(u_1,\cdots,u_{n-1}),u_n)$$

of $H_1\times\cdots\times H_n$ into H'' has the properties stated for f in Prop. 5, so that, by the unicity assertion in Prop. 5, H'' is isomorphic to H.

From this one deduces that every element $\mathfrak{H}$ of the group we have just described is of finite order. In fact, take on a space H of class $\mathfrak{H}$ any positive cycle $\sum_{i=1}^{n} a_i$ of dimension 0, rational over k. Call H_n any space of class $n\mathfrak{H}$; then there is a mapping $f(u_1,\cdots,u_n)$ of the product of n factors equal to H into H_n with the properties stated in Prop. 5. From the unicity assertion in Prop. 5, it follows that any permutation of the u_i will change f

into sf, with $s \in G$; as f is everywhere defined, we see that $s = e$ by taking $u_1 = \cdots = u_n$; therefore f is a symmetric function, so that $f(a_1, \cdots, a_n)$ is rational by the main theorem on symmetric functions (VA-7, Th. 1). So H_n has a rational point over k, and is therefore isomorphic to G.

Now, $\mathfrak{A}$ being as before, put $H_0 = G$ and take, for each integer $n \neq 0$, a space H_n of class $n\mathfrak{A}$ so that all the H_n are disjoint. On the set $\mathfrak{G} = \bigcup_n H_n$ (which is of course not an algebraic variety), we will define a commutative group-law f (in the sense of group-theory, not of algebraic geometry) such that $H_0 = G$ will be a subgroup of $\mathfrak{G}$ and that f induces on $H_m \times H_n$, for all m, n, a mapping $f_{m,n}$ of $H_m \times H_n$ into H_{m+n} satisfying the conditions in Prop. 5. As there is such a mapping $f_{m,n}$ for each m, n, and as it is uniquely determined up to an automorphism of H_{m+n} (i.e. up to left-multiplication by a rational point of G), we merely have to choose the $f_{m,n}$ so that the mapping f of $\mathfrak{G} \times \mathfrak{G}$ into $\mathfrak{G}$ which coincides with $f_{m,n}$ on $H_m \times H_n$ for all m, n satisfies the axioms for groups; we do this as follows. For any n, we take $f_{0,n}(x, u) = xu$ for $x \in G$, $u \in H_n$. We choose $f_{-1,1}$ and, for all $n > 0$, $f_{n,1}$ and $f_{-n,-1}$ so as to satisfy the conditions in Prop. 5. Now, for elements $u_1, \cdots, u_{n+1}$ of H_1 in any number, we define $u_1 \cdots u_{n+1}$ inductively as being equal to u_1 for $n = 0$ and to $f_{n,1}(u_1 \cdots u_n, u_{n+1})$ for $n \geqq 1$; similarly, for elements $v_1, \cdots, v_{n+1}$ of H_{-1}, we define $v_1 \cdots v_{n+1}$ as equal to v_1 for $n = 0$ and to $f_{-n,-1}(v_1 \cdots v_n, v_{n+1})$ for $n \geqq 1$. It is then easily seen that, whenever m, n are both > 0, there is one and only one way of choosing $f_{m,n}$ so that it satisfies the condition

$$f_{m,n}(u_1 \cdots u_m, u_{m+1} \cdots u_{m+n}) = u_1 \cdots u_{m+n}$$

when the u_i are in H_1; we determine $f_{-m,-n}$ similarly, using H_{-1} instead of H_1. Finally, for $m \geqq n > 0$, we choose $f_{m,-n}$ and $f_{-m,n}$ so as to satisfy the conditions

$$f_{m,-n}(u_1 \cdots u_m, v_1 \cdots v_n) = \prod_{i=1}^{n} f_{-1,1}(v_i, u_i) \cdot u_{n+1} \cdots u_m$$

$$f_{-m,n}(v_1 \cdots v_m, u_1 \cdots u_n) = \prod_{i=1}^{n} f_{-1,1}(v_i, u_i) \cdot v_{n+1} \cdots v_m$$

respectively, the u_i being any elements of H_1 and the v_i any elements of H_{-1}. It is then a trivial matter to verify that these choices of the $f_{m,n}$ satisfy all the requirements for a commutative group-law on $\mathfrak{G}$.

The points on the H_n which are rational over k form a subgroup $\mathfrak{g}$ of $\mathfrak{G}$. As we have shown that there are such points for some $n \neq 0$, there is a smallest $n > 0$ for which there is such a point $a \in H_n$; this n is the order of $\mathfrak{A}$ in the group of classes of principal homogeneous spaces with respect to G. Then $\mathfrak{g}$ is the direct product of the group $\mathfrak{g}_0 = \mathfrak{g} \cap G$ of rational

points over k on G and of the infinite cyclic group γ generated by a. The quotient-group $\mathfrak{G}/\gamma$ may be described as an algebraic group consisting of n components respectively isomorphic to $H_0 = G, H_1, \cdots, H_{n-1}$.

6. PROPOSITION 6. *Let A be an abelian variety and H a principal homogeneous space with respect to A, both being defined over a field k. Let $V_1, \cdots, V_n$ be varieties, and F a mapping of $V_1 \times \cdots \times V_n$ into H, all these being defined over k. Then there is for each i a principal homogeneous space H_i with respect to A and a mapping F_i of V_i into H_i, H_i and F_i being defined over k, and there is a mapping f of $H_1 \times \cdots \times H_n$ into H with the properties stated in Prop. 5, such that, for $(M_1, \cdots, M_n)$ generic over k on $V_1 \times \cdots \times V_n$, we have*

$$F(M_1, \cdots, M_n) = f(F_1(M_1), \cdots, F_n(M_n)).$$

Moreover, all these are uniquely determined up to isomorphisms.

For $n = 1$, there is nothing to prove. If the assertion is proved for a product of two factors, then this can be applied to the product $V_1 \times (V_2 \times \cdots \times V_n)$ of V_1 and $V_2 \times \cdots \times V_n$, so that the general case follows by induction on n. Thus it is enough to treat the case of two factors V, W and of a mapping F of $V \times W$ into H. Call ϕ the canonical mapping of $H \times H$ into A; let (M, N) and (M', N') be two independent generic points of $V \times W$ over k; and put

$$x = \phi(F(M, N'), F(M', N')), \qquad y = \phi(F(M, N), F(M, N')).$$

so that we have

$$xy = \phi(F(M, N), F(M', N')).$$

As the mapping $((M, M'), N') \to x$ of $(V \times V) \times W$ into A has the constant value e on the variety $(M, M) \times W$, Th. 7 of VA-18 shows that x is rational over $k(M, M')$; for a similar reason, y must be rational over $k(N, N')$; in other words, there are mappings Φ, Ψ of $V \times V$, $W \times W$ into A, both defined over k, such that $x = \Phi(M, M')$ and $y = \Psi(N, N')$. By the corollary of Th. 7 of VA-18, Φ and Ψ satisfy the assumptions of Prop. 4, so that there are two principal homogeneous spaces U_1, U_2 with respect to A, mappings F_1, G_1 of V into U_1 and mappings F_2, G_2 of W into U_2, all defined over k, such that $F_1(M) = xG_1(M')$, $F_2(N) = yG_2(N')$; moreover, as $\Phi(M, M)$, $\Psi(N, N)$ are defined and equal to e, we have $G_1 = F_1$, $G_2 = F_2$. Now call H_1, H_2 the spaces respectively opposite to U_1, U_2, and apply Prop. 5 to H_1, H_2: let $\bar{H}$ be the principal homogeneous space and $\bar{f}$ the mapping of $H_1 \times H_2$ into $\bar{H}$ with

the properties stated in that proposition. Put $\bar{F}(M,N) = \tilde{f}(F_1(M), F_2(N))$. As H_1, H_2 are opposite to U_1, U_2, we have

$$F_1(M') = xF_1(M), \qquad F_2(N') = yF_2(N),$$

multiplication in the right-hand sides being understood in the sense of H_1, H_2. By the definition of $\tilde{f}$, we have then:

$$\bar{F}(M',N') = (xy)\bar{F}(M,N),$$

while, as we have seen above, the same relation holds if F is substituted for $\bar{F}$. But then, as the corollary of Th. 7, VA-18, shows that the mapping

$$((M',N'),(M,N)) \to xy$$

of $(V \times W) \times (V \times W)$ into A satifies the condition of Prop. 4, the corollary of Prop. 4 shows that $\bar{H}$, $\bar{F}$ must be the same as H, F except for an isomorphism of H onto $\bar{H}$. Then, replacing $\tilde{f}$ by a mapping f of $H_1 \times H_2$ into H by means of that isomorphism, we have the spaces H_1, H_2 and the mappings F_1, F_2, f whose existence was asserted in our proposition.

As to unicity, assume that there are spaces H_1^*, H_2^* and mappings F_1^*, F_2^*, f^* with the same properties. Then, x being defined as above, or equivalently by $F(M',N') = xF(M,N')$, we have

$$f^*(F_1^*(M'),F_2^*(N')) = xf^*(F_1^*(M),F_2^*(N')) = f^*(xF_1^*(M),F_2^*(N'))$$

and therefore $F_1^*(M') = xF_1^*(M)$ since the mapping $u \to f^*(u,v)$ of H_1^* into H is, as easily seen, an everywhere biregular mapping of H_1^* onto H. But then the corollary of Prop. 4, applied to the mapping $(M',M) \to x$ of $V \times V$ into A, shows that H_1^*, F_1^* are the same as H_1, F_1 except for an isomorphism. The same argument applied to y instead of x shows that H_2, F_2 are uniquely determined up to an isomorphism. Then Prop. 5 shows that f is uniquely determined. This completes the proof.

7. The foregoing results will now be applied to the theory of Jacobian varieties. As in VA-35, we consider a complete non-singular curve Γ of genus $g > 0$, defined over a field k. If $\mathfrak{a}$ is any divisor on Γ, Prop. 6 of the Appendix of AG shows that there is a smallest field containing k over which $\mathfrak{a}$ is rational; this field will be denoted by $k(\mathfrak{a})$. In particular, if $M_1, \cdots, M_g$ are independent generic points of Γ over k and if we put $\mathfrak{m} = \sum_i M_i$, then, by VA-4, Lemma 1, $k(\mathfrak{m})$ is the field $k(M_1, \cdots, M_g)_s$ of symmetric functions of $M_1, \cdots, M_g$ defined over k, i.e. the subfield of $k(M_1, \cdots, M_g)$ consisting of those elements which are invariant under all permutations of

$M_1, \cdots, M_g$; such a divisor $\mathfrak{m}$ will be called generic over k. As $k(\mathfrak{m})$ is a regular extension of k, we may write it as $k(u)$, where u is a generic point of a variety W over k, and we may write $u = F(M_1, \cdots, M_g)$, with F defined over k; as F is symmetric in the M_i, this may also be written as $u = F(\mathfrak{m})$.

Now let the N_i, P_i, for $1 \leqq i \leqq g$, be $2g$ independent generic points of Γ over $k(\mathfrak{m})$; and put:

$$x = (N_1, \cdots, N_g, P_1, \cdots, P_g),$$

this being a generic point over k of the product $V = \Gamma \times \cdots \times \Gamma$ of $2g$ factors equal to Γ. By VA-35, Lemma 11, there is a positive divisor $\mathfrak{m}'$ on Γ linearly equivalent to $\mathfrak{m} + \sum_{i=1}^{g} N_i - \sum_{i=1}^{g} P_i$, and it is uniquely determined and such that $k(x, \mathfrak{m}) = k(x, \mathfrak{m}')$; this implies that it is generic over $k(x)$. Then, if we write $u' = F(\mathfrak{m}')$, we have $k(x, u) = k(x, u')$; we may thus write $u' = g(x, u)$, where g is a mapping of $V \times W$ into W which satisfies (TG 1).

We now show that this mapping satisfies the condition (TG 2′) of AG, no. 3. Prop. 2, so that this proposition may be applied to it. In fact, let y be a generic point of V over $k(x, u)$; we may write

$$y = (Q_1, \cdots, Q_g, R_1, \cdots, R_g).$$

Then the point $u'' = g(y, u')$ will be determined by $u'' = F(\mathfrak{m}'')$, where $\mathfrak{m}''$ is the positive divisor linearly equivalent to $\mathfrak{m}' + \sum_i Q_i - \sum_i R_i$. Applying again VA-35, Lemma 11, we see that there is a positive divisor $\sum_i S_i$ linearly equivalent to $\sum_i N_i - \sum_i P_i + \sum_i Q_i$, and that it is generic over $k(y, u)$ and rational over $k(x, y)$. But then $\mathfrak{m}''$ is linearly equivalent to $\mathfrak{m} + \sum_i S_i - \sum_i R_i$, which shows that, if we put

$$z = (S_1, \cdots, S_g, R_1, \cdots, R_g)$$

z is generic on V over $k(u)$ and that we have $u'' = g(z, u)$. This shows that g satisfies (TG 2′). Applying Prop. 2 of AG, no. 3 and the main theorem of AG, we see that there is a group J, a normal law $\bar{g}$ between J and W, and a mapping ϕ of V into J such that $g(x, u) = \bar{g}(\phi(x), u)$ for x, u generic and independent over k on V, W.

Put now $K = k(P_1, \cdots, P_g)$, $\mathfrak{n} = \sum_i N_i$, and

$$w = (S_1, \cdots, S_g, Q_1, \cdots, Q_g).$$

Since the P_i, Q_i, N_i are generic and independent over k, Lemma 11 of VA-35

shows that w is generic over K on V. At the same time, the linear equivalence by which the S_i were defined shows at once that $g(x,u)=g(w,u)$ for u generic over $k(x,w)$, and therefore $\bar{g}(\phi(x),u)=\bar{g}(\phi(w),u)$. Since J, by definition, operates faithfully on W, this implies $\phi(x)=\phi(w)$; as w is generic over K on V, this shows that $\phi(x)$ is generic over K on J. It will now be shown that $K(\phi(x))=K(\mathfrak{n})$. In fact, if u and $u'=g(x,u)$ are as before, u' is rational over $K(\mathfrak{m},\mathfrak{n})=K(u,\mathfrak{n})$ since the divisor $\mathfrak{m}'$ is so by Lemma 11 of VA-35; therefore the mapping $u\to u'$ is defined over $K(\mathfrak{n})$, so that $K(\phi(x))\subset K(\mathfrak{n})$. Put now $K'=K(\phi(x))$, so that u' is rational over $K'(u)$; then $\mathfrak{m}$ and $\mathfrak{m}'$ are both rational over $K'(u)$. But Lemma 11 of VA-35 shows that $\mathfrak{n}$ is rational over $K(\mathfrak{m},\mathfrak{m}')$ and therefore over $K'(u)$. If u_1 is a generic point of W over $K'(u)$, $\mathfrak{n}$ will also be rational over $K'(u_1)$; as $K'(u)$, $K'(u_1)$ are independent regular extensions of K', this implies that $\mathfrak{n}$ is rational over K'.

But now a comparison with the construction of the jacobian variety given in VA-36 shows that the latter coincides with our J over a suitably extended groundfield; more precisely, substituting K for k, $\sum_i P_i$ for $\mathfrak{a}$, $\mathfrak{n}$ for $\mathfrak{m}$ and $\phi(x)$ for z in the treatment given in VA-36, we get the same law of composition for the field $K(\phi(x))$ as has been defined above. Alternatively, one may also reason as follows. Let J_1 be the jacobian variety as defined in VA; let ϕ_1 be the "canonical mapping" of Γ into J_1, also according to the definition of VA-37 (which will soon be replaced by a more appropriate one); let K_1 be an overfield of the field K defined above, over which J_1 and ϕ_1 are defined; take $\mathfrak{n}$ generic over K_1; put $t=\phi(x)$, x being as above, and $z=S[\phi_1(\mathfrak{n})]$. As we have then $K_1(x)=K_1(z)=K_1(\mathfrak{n})$, the mapping $x\to z$ defines a birational correspondence between J and J_1, defined over K_1. If we write it as $z=f(x)$, f is everywhere defined by VA-15, Th. 6; and this, by the results at the beginning of VA-19, must then be of the form $f(x)=f_0(x)+a$, where $a=f(e)$ and where f_0 is a homomorphism, so that (using the additive notation on J_1 and the multiplicative notation on J) we have $f_0(xx')=f_0(x)+f_0(x')$. But then f_0 is again a birational correspondence, and, if g is the inverse mapping to f_0, we have $g(z+z')=g(z)g(z')$ for z, z' generic and independent over K_1 on J_1. This can be written as $g(z)=g(z+z')g(z')^{-1}$; if then z_1 is any point of J_1, and we take z' generic on J_1 over $K_1(z_1)$, this shows that g is defined at z_1. As f_0, g are everywhere defined, they determine an isomorphism between J and J_1.

One could also, without making use of the results of VA, verify directly (for instance by making use of the criterion for the completeness of a group

given by VA-33, Th. 16) that the group J we have constructed here is complete and is therefore an abelian variety. Then the results we have proved above, combined with the corollary of Th. 7, VA-18, show at once that J has the properties stated in VA-36, Th. 18; since the whole theory of the jacobian variety depends upon nothing else, and these properties (as proved in VA-37) are characteristic of the jacobian variety, this would suffice for a complete treatment.

From this discussion, we conclude that J is an abelian variety. Now apply Prop. 6 to the mapping ϕ of V into J; this defines $2g$ mappings of Γ into principal homogeneous spaces with respect to J, all defined over k. As ϕ is symmetric in the N_i and also in the P_i, the unicity assertion in Prop. 6 shows at once that the first g mappings must coincide, and that the last g mappings must coincide; call F, F' these mappings, and H, H' the spaces into which they map Γ. Now, notations being the same as above in no. 6, put

$$x' = (P_1, \cdots, P_g, N_1, \cdots, N_g).$$

Then we have, always with the same notations as before, $u = g(x', u')$, and therefore $\phi(x') = \phi(x)^{-1}$. This, combined with the unicity assertion in Prop. 6, shows at once that H' is the opposite space to H while F' must be the same as F.

We now embed J and H, in the manner explained at the end of no. 5, into a commutative group $\mathfrak{G}$ consisting of principal homogeneous spaces H_n with respect to J, all defined over k, with $H_0 = J$, $H_1 = H$, in such a way that $\mathfrak{G}/J$ is an infinite cyclic group, that the H_n are the cosets of J in $\mathfrak{G}$ and that the group-law in $\mathfrak{G}$ induces on $H_m \times H_n$, for all m, n, a mapping of $H_m \times H_n$ into H_{m+n} defined over k and satisfying the conditions in Prop. 5. At the same time, we change from the multiplicative to the additive notation, not only in J but also in $\mathfrak{G}$. With this notation, we have, if x, $\phi(x)$ and F have the same meaning as before,

$$\phi(x) = \sum_i F(N_i) - \sum_i F(P_i).$$

Let us now extend the mapping F into a homomorphism of the group of divisors on Γ into $\mathfrak{G}$, by putting $F(\mathfrak{a}) = \sum_i n_i F(A_i)$ for any divisor $\mathfrak{a} = \sum_i n_i A_i$, so that $F(\mathfrak{a}) \in H_n$ if n is the degree of $\mathfrak{a}$; in particular, $F(\mathfrak{a})$ is in J if and only if $\mathfrak{a}$ is of degree 0. If a is any point of H and M is a generic point of Γ over $k(a)$, the mapping $M \to F(M) - a$ of Γ into J, which is defined over $k(a)$, is a "canonical mapping" in the sense of VA-37; naturally it is only defined up to an additive constant; and, by the unicity assertion in Prop. 6,

no such mapping can be defined over k unless H is isomorphic to G, i. e. unless H has a rational point over k. From Th. 19 of VA-38, one deduces immediately that a divisor $\mathfrak{a}$ on Γ is linearly equivalent to 0 if and only if $F(\mathfrak{a}) = 0$.

In other words, *the homomorphism* $\mathfrak{a} \to F(\mathfrak{a})$ *determines an isomorphism of the group of all divisor-classes* (of any degree) *on* Γ *onto the group* $\mathfrak{G}$. From the foregoing results, one concludes easily that these properties are characteristic for $\mathfrak{G}$ and F, up to isomorphisms on J and its cosets H_n in $\mathfrak{G}$. One may call $\mathfrak{G}$ the *Jacobian group of* Γ, and F the *canonical mapping* of Γ, and of the group of divisors on Γ, into the Jacobian group. In substance, the construction of the varieties H_n has already been given by Chow (in [1]) by a method belonging to projective geometry.

THE UNIVERSITY OF CHICAGO.

BIBLIOGRAPHY.

[1] W. L. Chow, "The Jacobian variety of an algebraic curve," *American Journal of Mathematics*, vol. 76 (1954), pp. 453-476.

[2] S. Nakano, "Note on group varieties," *Memoirs of the College of Science, University of Kyoto*, Series A, vol. 27 (1952), Math. no. 1, pp. 55-66.

[3] A. Weil, *Variétés abéliennes et courbes algébriques*, Paris, Hermann et Cie, 1948.

[4] ———, "On algebraic groups of transformations," *American Journal of Mathematics*, vol. 77 (1955), pp. 355-391.

A PROOF OF A THEOREM OF MEYER ON INDEFINITE TERNARY QUADRATIC FORMS.*

By Burton W. Jones and Donald Marsh.

---

1. Introduction.[1] We shall be considering in this paper primitive indefinite ternary quadratic forms $f = \sum_{i,j=1}^{3} a_{ij}x_ix_j$ where the a_{ij} are integers with g. c. d. 1. We call J the g. c. d. of the two-by-two minor determinants of (a_{ij}) and $\det(a_{ij}) = J^2K$ defines an invariant K. (Classically these invariants were denoted by Ω and Δ). The purpose of this paper is to give a proof of the following theorem of A. Meyer [4] which is very fundamental in the theory of quadratic forms.

Theorem A. *If two primitive indefinite ternary quadratic forms are in the same genus and if their invariants J and K have g. c. d 1 or 2 and neither is divisible by 4, then the two forms are equivalent.*

Meyer gave what he called a proof of this theorem but which contained various obscurities which neither L. E. Dickson [1] nor the authors have been able to resolve. Bachmann did little to clarify these obscurities. L. E. Dickson gave a proof of Meyer's theorem (cf. [1], pp. 35-60) which was very involved in detail and had a few obscurities of its own, though it was an improvement over Meyer's discussion. Oral communication with Martin Eichler and Martin Kneser indicates that this theorem may also be proved using the deep theory of "spinor genera" developed by the former [2].

In this paper, by free use of matrices and the modern theory of quadratic forms including the Hasse symbol, we present a proof which involves a minimum of detailed computation and which we hope is largely free from obscurities.

The outline of the proof is as follows: Theorems 1 and 2 show that two ternary forms are equivalent if they have the same invariants J and K, if they are both properly or both improperly primitive and if they represent a binary form with certain properties. Theorem 3 gives two conditions under which a ternary form f represent all binary forms of determinant JM where

---

* Received February 11, 1955.

[1] This was written under the support of the Office of Naval Research.

M is a prime or double a prime according as the reciprocal form of f is properly or improperly primitive. Theorems 4, 5, 6, and 7 establish the satisfaction of the first of these conditions and Theorem 8 the second. The remainder of the proof is concerned with showing that any two forms of the same genus represent a binary form of determinant JM where M has the required properties.

THEOREM 1. *Let $B=(b_{rs})$ be the matrix of a properly or improperly primitive binary form, h, of determinant JM and let K be an integer such that $g=(M,K)$ is square-free and prime to both M/g and K/g; then there exists a ternary form f with invariants J and K which represents h primitively if and only if there are integers c_1 and c_2 such that*

$$(1) \qquad c_1^2 \equiv -b_{11}K, \qquad c_2^2 \equiv -b_{22}K, \qquad c_1c_2 \equiv +b_{12}K, \qquad (\mathrm{mod}\, M).$$

Proof. Let A be the matrix of the form f. The f represents h primitively if and only if there is a 3 by 2 integral matrix P whose two-rowed minor determinants have g. c. d. 1 and for which $P^TAP=B$. Then there is an integral column matrix Q such that $U=(P,Q)$ is a unimodular matrix and

$$U^TAU=E=(b_{ij}), \qquad i,j=1,2,3.$$

That is, f represents h if and only if it is equivalent to a form of matrix E whose leading two-by-two minor is B.

First suppose f with invariants J and K represent h, where JM is the determinant of h and (b_{ij}) is the matrix of $h, i,j=1,2$. Then write $\mathrm{adj}E=(B_{ij})$ where $B_{33}=JM$ and $B_{ij}\equiv 0(\mathrm{mod}\, J)$ for all i,j. Now $\mathrm{adj}(\mathrm{adj}\, E)=J^2KE$. Hence

$$(2) \qquad B_{22}B_{33}-B^2{}_{23}=J^2Kb_{11},$$

$$(3) \qquad B_{11}B_{33}-B^2{}_{13}=J^2Kb_{22},$$

$$(4) \qquad B_{12}B_{33}-B_{13}B_{23}=-J^2Kb_{12},$$

which show that we may take $c_1=B_{23}/J$, $c_2=B_{13}/J$ and have the congruences (1).

Conversely, if the congruences (1) hold equations (2), (3), (4) with $c_1=B_{23}/J$, $c_2=B_{13}/J$ are solvable for B_{22}, B_{11} and B_{12}. Thus the matrix (B_{ij}) exists. Suppose the elements B_{ij}/J had a common prime factor q. Then q^2 would divide Kb_{11}, Kb_{22}, Kb_{12} and since $(b_{11},b_{22},b_{12})=1$, q^2 would divide K. But $B_{33}=JM$ and hence $q\,|\,M$. However q would not be prime to (M,K) unless q^2 divides M which is impossible since (M,K) is square-free. Thus 1 is the g. c. d. of B_{ij}/J. A little calculation shows that J^4K^2 is

the determinant of (B_{ij}). Then $\mathrm{adj}(B_{ij})/J^2K$ is equal to a matrix E whose leading two-by-two minor is B and which has the invariants J and K.

Let us henceforth take $(J,K) \leqq 2$, $J \not\equiv 0 \not\equiv K \pmod 4$, and let $w = 1$ or 2 as f is properly or improperly primitive. Notice that if $w = 2$, $K \equiv 2 \pmod 4$ and J is odd.

THEOREM 2. *Two ternary quadratic forms of the same invariants, J, K and w, are equivalent if they both represent primitively the same primitive binary form of determinant JM in which M is an odd prime or twice an odd prime such that $(M,K) = g$ and $(g, K/g) = 1$.*

Proof. For M a prime or twice a prime and $(g, K/g) = 1$, the preceding theorem holds and the congruential conditions (1) have only the pair of solutions c_1, c_2 and the corresponding $-c_1$, $-c_2$, modulo M. The corresponding ternary forms obtained are related by the transformation $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$, whereas the form obtained by using $c_1 + tM$, $c_2 + uM$ with t, u integers in place of c_1, c_2 is related to the latter by means of the unimodular transformation

$$\begin{pmatrix} 1 & 0 & -u \\ 0 & 1 & -t \\ 0 & 0 & 1 \end{pmatrix}.$$

We now seek to determine conditions under which the hypothesis of Theorem 2 holds.

2. THEOREM 3. *If a ternary form f represents a primitive binary form $-h$ of determinant JM where M is a prime or double a prime according as the reciprocal form of f is properly or improperly primitive, and if h' is another binary form of determinant JM, then f represents $-h'$ if there are two primes p and q not dividing $2M\,|\,f\,|$ such that*

(i) *If T, U is the least solution of $x^2 - wpqKy^2 = 1$, then $T \not\equiv \pm 1 \pmod{wpq}$.*

(ii) *The equations $h = wpq$, $h' = wpq$ are both solvable.*

Proof. Consider h and h' as having been transformed so that their leading coefficients are wpq and let $B = (b_{rs})$ be the matrix of h with $b_{11} = wpq$. Since p, q do not divide M, b_{12} is prime to b_{11} and is one of the four roots of $x^2 \equiv -JM \pmod{wpq}$. If we show that some unimodular transformation of f leaves b_{11} and $|\,B\,|$ fixed, but replaces b_{12} by $b_{12}' \not\equiv \pm b_{12}$

$(\text{mod } wpq)$, then f represents $-h'$ since the "b_{12}" for h' is one of b_{12}, b_{12}', $-b_{12}$, $-b_{12}'$.

Write the matrix of f in the form (a_{rs}) where $a_{11} = -b_{11}$, consider the reciprocal form and denote

$$\begin{pmatrix} A_{22} & A_{23} \\ A_{23} & A_{33} \end{pmatrix}$$

by R. The determinant of R is $-b_{11}K$. If P is an automorph of R, then the transformation $\begin{pmatrix} 1 & 0 \\ 0 & P \end{pmatrix}$ on F is equivalent to the transformation $\begin{pmatrix} 1 & 0 \\ 0 & P^{IT} \end{pmatrix}$ on f (leaving b_{11} and $b_{11}K$ invariant). P^I is of the form

$$\begin{pmatrix} t - A_{23}u & -A_{33}u \\ A_{22}u & t + A_{23}u \end{pmatrix}$$

where t, u is a solution of $x^2 - wpqKy^2 = 1$. Now

$$b_{12}' = (a_{12}, a_{13}) \begin{pmatrix} t - A_{23}u \\ -A_{33}u \end{pmatrix} = a_{12}t - u(a_{12}A_{23} + a_{13}A_{33})$$
$$\equiv a_{12}t - u(a_{11}A_{31} + a_{12}A_{32} + a_{13}A_{33}) \equiv a_{12}t \ (\text{mod } wpq).$$

Thus $b_{12}' \equiv b_{12}t \ (\text{mod } wpq)$ and, if $t \not\equiv \pm 1 \ (\text{mod } wpq)$, then $b_{12}' \not\equiv \pm b_{12} \ (\text{mod } wpq)$.

We now find the conditions which must be imposed on p and q if (i) and (ii) of Theorem 3 are to hold. First in the next four theorems we show that if the product pq satisfies certain conditions $(\text{mod } 8)$ and $(\text{mod } K)$, and if for some fixed factor d_0 of K, p satisfies the condition $(-d_0 \mid p) = -1$, then

$$x^2 - aKy^2 = 1, \qquad a = wpq \tag{5}$$

has a minimum solution T, U with $T \not\equiv \pm 1 \ (\text{mod } wpq)$.

THEOREM 4. *If $K = 2^eG^2H$ where GH is odd, H square-free, $(a, K) \leqq 2$ and a is odd or double an odd according as $w = 1$ or $w = 2$, and $T^2 - aKU^2 = 1$ with $T \equiv \pm 1 \ (\text{mod } a)$, then for some factorization dd' of H with d, d' relatively prime and positive, the following equation has a solution where cc' is the highest power of 2 in 2^eU^2 and not both c, c' are divisible by 4:*

$$dcx^2 - d'c'ay^2 = \pm 2. \tag{6}$$

Proof. Equation (5) implies $(T \mp 1)(T \pm 1) = 2^eaG^2HU^2$ and $T \equiv \pm 1 \ (\text{mod } a)$ implies

$$T \mp 1 = ad'c'r_1^2, \qquad T \pm 1 = dcr_2^2, \qquad (r_1, r_2) = 1, \tag{7}$$

since $T \mp 1$ and $T \pm 1$ have at most a factor 2 in common, where r_1 and r_2 are odd, $r_1^2 r_2^2 cc' = 2^e G^2 U^2$ and $dd' = H$. Subtracting the first equation of (7) from the second, we have

$$(T \pm 1) - (T \mp 1) = \pm 2 = dcr_2^2 - ad'c'r_1^2, \tag{8}$$

which completes the proof.

Since equations (6) differ according to the parity of e, we specialize these results to find

(1) If $e = 0$, c and c' may both be 1 or one is 2 and the other an odd power of 2 greater than the first; in the former case the equation (6) becomes

$$dx^2 - d'ay^2 = \pm 2. \tag{6_1}$$

If c and c' are both even, we have

$$dx^2 - d'ay^2 = \pm 1 \tag{6_2}$$

where x or y is even.

(2) If $e = 1$, one of c, c' is 2 and the other is an even power of 2. Then (8) becomes $\pm 1 = dr_2^2 - 2ad'(\frac{1}{2}\sqrt{c'})^2 r_1^2$ or $\pm 2 = d(\sqrt{c})^2 r_2^2 - 2ad' r_1^2$; hence we have one of

$$dx^2 - 2ad'y^2 = \pm 1, \tag{6_3}$$

$$dx^2 - 2ad'y^2 = \pm 2. \tag{6_4}$$

We show that by proper choice of a modulo the primes dividing G but not H we may exclude from consideration equations (6_2) and (6_3) with $d = 1$, and $\pm 1 = 1$. Note that $d = 1$ implies $d' = H$.

THEOREM 5. *If, according as e is 0 or 1, a or $2a$ is so chosen that $(-aH \mid p_i) = -1$ or $(-2aH \mid p_i) = -1$ for all primes p_i dividing G but not H, then, if T, U is the least solution of (5), it follows that if $T \equiv \pm 1 \pmod{a}$ then (6) does not reduce to either of the following in the respective cases:*

$$x^2 - aHy^2 = 1, \qquad x^2 - 2aHy^2 = 1. \tag{9}$$

Proof. Suppose for the least solution T, U equations (7) with $d = 1$, $d' = H$ define r_2, r_1 a solution of (6_2) or (6_3) with $d = 1$ and $\pm 1 = 1$, that is, a solution of one of the equations (9). First we take the case $r_1 = Gr$ and show that T, U is not the least solution of (5). For $e = 0$, $x_0 = r_2(\frac{1}{2}c)^{\frac{1}{2}}$, $y_0 = r_1(\frac{1}{2}c')^{\frac{1}{2}}$ in (9) gives $x_0^2 - aG^2H(y_0/G)^2 = 1$; $x_0, y_0/G$ is a solution of (5) in which $T = cr_2^2 - 1$ and $x_0 = r_2\sqrt{(\frac{1}{2}c)} < T$ which yields our contradiction.

If $e=1$, $r_1=Gr$ implies that $x_0=r_2$, $y_0=(\frac{1}{2}\sqrt{c'})r$ is a solution of (9) with $x_0<T$.

Second, suppose that $r_1\not\equiv 0 \bmod G$), thus $r_1r_2\equiv 0 \pmod G$ implies that r_2 contains a prime factor of G and (6_3) and (6_2) with $d=1$, $d'=H$ implies that the prime factors of G which r_2 contains cannot divide H. For (9) to have no solutions with x divisible by a prime factor of G not dividing H it is therefore sufficient that $(-aH\,|\,p_i)=-1$ or $(-2aH\,|\,p_i)=-1$ in the respective cases for all primes p_i dividing G but not H. This completes the proof.

We now consider equations

$$g=dx^2-bd'y^2=N, \tag{10}$$

where $b=a$ or $2a$ according as $e=0$ or 1, with aw^{-1} prime to $2H$ and N is prime to H. In order that (10) be solvable, it is necessary that $c_{p_i}(g)=(-N,bH)_{p_i}$ for all primes p_i, where $c_p(g)$ is the Hasse symbol (see [3], p. 47). We now choose $b \pmod H$ so that, for any fixed N prime to H, there is one and only one value of d such that $c_{p_i}(g)=(-N,bH)_{p_i}$ for all primes p_i dividing H.

THEOREM 6. *Let $p_1,p_2,\cdots,p_n$ be the prime factors of H. We can choose $b \pmod{p_i}$ $i=1,2,\cdots,n$ so that, for any N prime to H, there will be one and only one d dividing H such that*

$$c_{p_i}(g)=(-N,bH)_{p_i} \tag{11}$$

for all primes p_i dividing H.

Proof. First compute $c_p(g)$ and find it equal to $(-1,bH)_p(d,bH)_p=(-d,bH)_p$. Suppose $(-d_1,bH)_p=(-d_2,bH)_p$ for all such p. This implies and is implied by $(d_1d_2,bH)_p=1$ for such p. Hence our theorem will be proved if we can show that, for a proper choice of b, $(d,bH)_p=1$ for all p dividing H holds for one and only one value of d (namely $d=1$).

In order to prove this by induction, assume first that H is a prime; then the two possible values of d are 1 and p. Since $(1,bp)_p=1$, we want to choose b so that $(p,bp)_p=-1$. Now $(p,bp)_p=(p,-b)_p=(-b\,|\,p)$. Hence choose b so that the latter is -1.

Assume the theorem for H containing prime factors $p_1,p_2,\cdots,p_{n-1}$ and that b has been chosen so that $(d,bH)_p=1$ for all primes dividing H only when $d=1$. In order to establish the theorem for p_nH choose b' so that $(b'p_n\,|\,p_i)=(b\,|\,p_i)$ for $i=1,2,\cdots,n-1$. We must show that for $d\neq 1$ neither of the following is 1 for $p_i=p_1,p_2,\cdots,p_n$: $(d,b'Hp_n)_{p_i}$, $(dp_n,b'Hp_n)_{p_i}$.

First, $(d, b'Hp_n)_{p_i} = (d, bH)_{p_i}$ for $i = 1, 2, \cdots, n-1$ and since the latter is -1 for some i, the former is also. Second, $(dp_n, b'Hp_n)_{p_i} = (dp_n, bH)_{p_i}$ for $i = 1, 2, \cdots, n-1$ and the latter symbol is equal to $(d, bH)_{p_i}(p_n, bH)_{p_i}$; thus, if $(dp_n, b'Hp_n)_{p_i} = 1$ for $i = 1, 2, \cdots, n$ we have $(d, bH)_{p_i} = (p_n, bH)_{p_i}$ for $i = 1, 2, \cdots, n-1$. Thus, by the hypothesis of our induction, there is one and just one d, i.e., d_0, which has this property. Then, choose b' (mod p_n) so that $(d_0p_n, b'Hp_n)_{p_n} = -1$. This is possible since $(d_0p_n, b'Hp_n)_{p_n} = (d_0, b'Hp_n)_{p_n}(p_n, b'Hp_n)_{p_n} = (d_0 | p_n)(-b'H | p_n)$. Since for $d = 1$, $c_p(g) = (-1, bH)_p$ for all primes dividing H, the above shows that we need not consider (10) with $N = 1$ for $d \neq 1$. Theorem 5 shows that proper choice of a (mod G) also excludes $N = 1$, $d = 1$. This completes the proof and we complete the exclusion of (10) by the following theorem.

THEOREM 7. *There exist odd numbers α, β incongruent* (mod 4), *a divisor d_0 of H, and a choice of sign $\pm$ so that* (10) *with $N = -1, 2, -2$ have no solutions for the following conditions imposed upon a:*

(1) *If $e = 0$, $aH \equiv 1$ (mod 4) or $aH \equiv 5 \pm 2$ (mod 8),*

(2) *If $e = 1 = w$, $aH \equiv \alpha$ or β (mod 8),*

(3) *$a = wpq$ where p and q are distinct primes not dividing $2H$ and $(-d_0 | p) = -1$.*

Proof. If $e = 0$, we may assume from the previous theorem that a is chosen (mod K) so that for all p_i dividing H each of the following three equations is solvable in $R(p_i)$ for only one divisor d of H:

(12) $dx^2 - a(H/d)y^2 = -1$, $dx^2 - a(H/d)y^2 = +2$, $dx^2 - a(H/d)y^2 = -2$;

that is,

(13) $(-d, aH)p_i = 1$, $(2d, aH)p_i = 1$, $(-2d, aH)p_i = 1$ for all p_i dividing H.

Let the respective values of d be d_1, d_2, d_3. First, if $aH \equiv 1$ (mod 4), the last two equations of (12) have no solution and we may exclude the first by choosing p so that $(-d_1, aH)_p = (-d_1 | p) = -1$. Second, consider $aH \equiv 3$ (mod 4). Now $(-d_1, aH)_{p_i} = (2d_2, aH)_{p_i} = 1$ implies $(-2d_1d_2, aH)_{p_i} = 1$ for all p_i dividing H. Since there is just one divisor d_3 of H such that $(-2d_3, aH)_{p_i} = 1$ for all p_i dividing H, d_1d_2 is, except for a square factor, equal to d_3. Similarly, any product of two of d_1, d_2, d_3 is, except for a square factor, equal to the third. This implies that at least one of d_1, d_2, d_3 is congruent to 1 (mod 4). Suppose $-d_1 \equiv -1$ (mod 4), then $aH \equiv 3$ (mod 4) implies $(-d_1, aH)_2 = -1$ and one of $(2d_2, aH)_2$, $(-2d_3, aH)_2$ is -1. Sup-

pose that it is the former. Then choose p so $(-2d_3, aH)_p = (-2d_3 | p) = -1$.

If $e = 1 = w$, we have the same set of equations except that a is replaced by $2a$. There are two odd numbers α such that $(2d_2, 2\alpha)_2 = (2d_2, 2)_2(2d_2, \alpha)_2 = -1$ and the two are incongruent (mod 4). Make $aH \equiv \alpha \pmod 8$ and see that two of the equalities in (13) are denied for $p_i = 2$ and the third may be denied for $p_i = p$.

If $e = 1$, $w = 2$ equation (10) becomes $N = dx^2 - 4pqd'y^2$ which is not solvable for $N = 2$ or -2. The other equation is excluded by $(-d_0 | p) = -1$ where d_0 is the value of d for $N = -1$.

Theorems 5, 6 and 7 list restrictions imposed on p and q (mod $8K$) which assure the satisfaction of condition (i) of Theorem 3. We now consider condition (ii) of Theorem 3.

THEOREM 8. *Let h and h' be binary forms of the same primitive genus and of determinant JM; let d_0 be some integer prime to $2JM$ and $(JM, K) \leqq 2$; let h represent an integer a_0 satisfying the conditions* (mod $16K$) *imposed by Theorems 5, 6 and conditions 1 and 2 of Theorem 7. Then there are two primes p and q such that $(-d_0 | p) = -1$, wpq is represented by h and h', and $wpq \equiv a_0 \pmod{16K}$.*

Proof. We carry through the proof for h properly primitive. If h and h' are improperly primitive the same proof holds if we replace h and h' by $\frac{1}{2}h$ and $\frac{1}{2}h'$. This of course replaces JM by $\frac{1}{4}JM$.

The form hh' derived by composition from h and h' is in the principal genus and hence arises by duplication (cf. [3], p. 167); hence $hh' = v^2$ and, denoting the class vh'^{-1} by u, we have $h' = vu^{-1}$. Since d_0 is an odd factor of K and JM is the determinant of v with $(K, JM) \leqq 2$, there is an integer p' prime to $2 | f | M$ such that $(-d_0 | p') = -1$ and p' is compatible with the characters of v. For any a compatible with the characters of h and prime to JM we can find an integer q' prime to $2 | f | M$ so that $p'q' \equiv a \pmod m$ for any preassigned m prime to p'. Then v represents infinitely many primes $p \equiv p' \pmod{8 | f | M}$ and thus u and u^{-1} infinitely many primes $q \equiv q' \pmod{8 | f | M}$. Let p, q be one such pair and have $h = pq$, $h' = pq$ both solvable.

The preceding theorems combine to establish the following result.

THEOREM 9. *If an indefinite primitive ternary form f represents primitively a primitive form $-h$ of determinant JM with $(JM, K) \leqq 2$, then it represents every binary form in the same genus as $-h$ provided*

(i) *M is an odd prime or twice a prime according as the reciprocal form of f is properly or improperly primitive.*

(ii) *h represents an integer a satisfying the conditions* (mod $8K$) *of Theorems 5, 6 and 7.*

Then in view of this theorem and Theorem 2, the proof of Meyer's theorem will be completed if we establish

THEOREM 10. *If f and f' are two indefinite primitive ternary forms of the same genus, if $(J, K) \leqq 2$ and neither J nor K is divisible by 4, then they represent, respectively, two primitive binary forms $-h$ and $-h'$ having the following properties:*

(i) *h and h' are the same genus and have determinant JM,*

(ii) *M is a prime not dividing $2JK$ or twice such a prime according as the reciprocal form of f is properly or improperly primitive,*

(iii) *h represents an integer a satisfying conditions 1 and 2 of Theorem 7.*

Theorems 5 and 6 need not be considered here since $(JM, K) \leqq 2$, implies that h represents integers $\equiv a \pmod{p}$ for any odd prime p dividing K.

The proof of this theorem requires two lemmas.

LEMMA 1. *Let the invariants, J, K and w, of a primitive indefinite ternary form f be such that $(J, K) \leqq 2$, $J \not\equiv 0 \not\equiv K \pmod 4$ and $w = 1$ or 2 according as the form f is properly or improperly primitive and, except for the factor 2, M is prime to JK. Then f represents a binary form $-h$ such that $h = a$ is solvable for a satisfying conditions 1 and 2 of Theorem 7 if M satisfies the following conditions exhibited in tabular form, where p. p. means properly primitive and i. p. means improperly primitive.*

Invariants	Conditions on M	Numbers represented (mod 8) by h
1. f p. p., J odd, K even	$M \equiv -J \pmod 4$ and $c_2(f) = (2 \mid -JM)$	arbitrary
2. F p. p., K odd, J even	arbitrary $JM \equiv \mp 2c_2(f) \pmod 8$	$a \equiv H \pmod 4$ and $c_2(f) = (2 \mid aH)$ $aH \equiv 5 \pm 2 \pmod 8$
3. f i. p., J odd, K even	arbitrary	$a \equiv 2$ or $6 \pmod 8$
4. F i. p., K odd, J even	$M \equiv J \pmod 8$	$a \equiv K \pmod 4$
5. JK odd	$c_2(f) = 1$ and $M \equiv 3J \pmod 8$ $c_2(f) = -1$ and $M \equiv J \pmod 4$	arbitrary $a \equiv -H \pmod 4$
6. $J \equiv K \equiv 2 \pmod 4$	$c_2(f) = (2\alpha, -JM)_2$ $c_2(f) = (2\beta, -JM)_2$	$a \equiv \alpha H \pmod 8$ $a \equiv \beta H \pmod 8$

(α and β defined in Theorem 7)

Proof. Since there are no requirements imposed by Theorem 7 for f improperly primitive, we need consider only properly primitive forms f in this proof. First we show that under the conditions imposed, f represents a primitive binary form $-h$ of determinant JM. Let g be the greatest odd factor common to all the coefficients of h. Then $g^2 | J$ and, since J and M have no odd factors in common, we may by an equivalence transformation on F have

$$F \equiv cJKx^2 + bKy^2 + Mz^2 \pmod{J_0^2},$$

where J_0 is the greatest odd factor of J and bc is prime to J_0. Then

$$f \equiv bMx^2 + cJMy^2 + bcJKz^2 \pmod{J_0^2},$$

and the leading binary of f has determinant JM and leading coefficient congruent (mod g^2) to bM which is therefore prime to g. Thus the coefficients of this leading binary form have no odd prime factor in common. This shows that h may be taken to be primitive.

To show that h is properly primitive notice first that it can be improperly primitive only if $JM \equiv 3 \pmod 4$ or $4 \pmod 8$. We postpone the latter and consider the former. If, under this condition, it is improperly primitive, it can be considered to have a leading element $-2s \equiv 2 \pmod 4$. Then

$$c_2(f) = (-2sK, -JM)_2. \tag{14}$$

If K is odd, then by the conditions imposed on M either $c_2(f) = 1$ in which case $JM \equiv 3 \pmod 8$ implies $(-2sH, -JM)_2 = -1 \neq c_2(f)$, or $c_2(f) = -1$ and $JM \equiv 1 \pmod 4$. Thus, for K odd, condition 5 of the lemma implies that f represents no improperly primitive forms of determinant JM. If $K \equiv 2 \pmod 4$ and f represents an improperly primitive binary h of determinant JM, then f may be taken congruent to $h + cx_3^2 \pmod{2^r}$ with c even, which denies f properly primitive. It remains to consider the numbers which h represents and $JM \equiv 4 \pmod 8$.

If $JM \not\equiv 0 \pmod 4$, the numbers (mod 8) which h represents will be determined by its Hasse symbol with $p = 2$. Furthermore h represents a (mod 8) if and only if $c_2(f) = (aK, -JM)_2$. Now consider the conditions in order.

1. Here $M \equiv -J \pmod 4$ shows that $c_2(f) = (2 | -JM)$ and all odds (mod 8) are represented by h.

2. Here the numbers a represented by h are given by $c_2(f) = (aH, -JM)_2$. Thus if $aH \equiv 1 \pmod 4$, a is represented if and only if $c_2(f) = (aH, -JM)_2$

$= (2|aH)$ regardless of the choice of M. If $aH \equiv 5 \pm 2 \pmod 8$ the choice of $M \pmod 4$ specified suffices.

3. If f is improperly primitive, Theorem 7 imposes no restrictions.

4. If $M \equiv J \pmod 8$, h represents numbers congruent to $K \pmod 4$ and is properly primitive, for F may be taken congruent to

$$g + 2cx_3^2 \pmod{2^r},$$

where g is an improperly primitive binary form. Kf is then congruent to $2g_1 + ex_3^2 \pmod{2^r}$, where $e \equiv -1 \pmod 4$, and g_1 is an improperly primitive binary form. However g_1 cannot have determinant $JM/4$ since the condition imposed requires $JM/4 \equiv 1 \pmod 4$. This shows that f does not represent an improperly primitive binary form of determinant $JM/4$. On the other hand, the odd numbers represented by Kf are congruent to e, that is, congruent to $-1 \pmod 4$. This shows that the odd numbers represented by h are congruent to $K \pmod 4$.

5. If $c_2(f) = 1$ and $JM \equiv 3 \pmod 8$, then $c_2(f) = (aH, -JM)_2$ for a arbitrary. But $c_2(f) = -1$ and $JM \equiv 1 \pmod 4$ shows that $-1 = (aH, -1)_2$ and hence $aH \equiv -1 \pmod 4$.

6. Here $a \equiv \alpha H \pmod 8$ if and only if $c_2(f) = (2\alpha, -JM)_2$. This completes the proof.

Our final step in the proof of Theorem 10 and hence of Meyer's theorem is

LEMMA 2. *If the invariants J, K and w satisfy the conditions of the theorem and if f and f' are indefinite forms of the same primitive genus with these invariants, then F and F', their reciprocal forms, represent a prime M or twice such a prime satisfying the conditions imposed on M in Lemma* 1.

Proof. Since the classes f and $-f$ are class isomorphic, for this lemma we take J and K to be negative integers. This makes the binary h and the binary g, determined below, indefinite forms and therefore capable of representing both positive and negative integers.

If the form f represents wq where q is a prime not dividing $2|f|$ then, by Theorem 9 with f and F interchanged, F represents a binary form $-g$ of determinant qK and all binaries in the genus of $-g$ and hence all numbers $-r$, where r is consistent with the generic characters of g, provided conditions 1 and 2 of Theorem 7 hold after replacing a, J and K by $-r$, K and J respectively, that is

1′) If J is odd, $-rJ \equiv 1 \pmod 4$ or $-rJ$ congruent to a preassigned one of 3, 7 (mod 8).

2′) If J is even, F properly primitive, $-rJ/2 \equiv \alpha_1$ or $\beta_1 \pmod 8$ for α_1 and β_1 preassigned with $\alpha_1\beta_1 \equiv -1 \pmod 4$.

By Lemma 1 with f and F, a and $-r$ interchanged, the representation of such an r by F will be assured by the following choices of wq exhibited in tabular form. (Note that $c_2(f) = c_2(F)$.)

Invariants	Conditions on q	Conditions (mod 8) on r
f p. p., J odd, K even	arbitrary	$-r \equiv J \pmod 4$ and $c_2(f) = (2\mid -rJ)$
	$Kq \equiv \mp 2c_2(f) \pmod 8$	$-rJ \equiv 5 \pm 2 \pmod 8$
F p. p., J even, K odd	$q \equiv -H \pmod 4$ and $c_2(f) = (2\mid -qH)$	arbitrary
f i. p., J odd, K even	$q \equiv H \pmod 4$	$-r \equiv J \pmod 4$
F i. p., J even, K odd	arbitrary	$r \equiv 2$ or $6 \pmod 8$
JK odd	$c_2(f) = 1$ and $q \equiv 3H \pmod 8$	arbitrary
	$c_2(f) = -1$ and $q \equiv H \pmod 4$	$-r \equiv -J \pmod 4$
$J \equiv K \equiv 2 \pmod 4$	$c_2(f) = (2\alpha_1, -Kq)_2$	$-r \equiv \alpha_1 J/2 \pmod 8$
	$c_2(f) = (2\beta_1, -Kq)_2$	$-r \equiv \beta_1 J/2 \pmod 8$

First, to show that such a choice of wq is possible, notice ([3], p. 87), f properly primitive implies that f represents all odds (mod 8) unless K is odd and $c_2(f) = -1$. In this case the only odds excluded (mod 8) are those numbers b for which $bH = -1 \pmod 8$. Inspection of the table shows that choice of q may be made consistent with this exclusion. Similarly if f is improperly primitive $2q$ is excluded (mod 8) only when $c_2(f) = -1$ and $qH \equiv -1 \pmod 8$, where the corresponding entry in the table is $q \equiv H \pmod 4$.

Next, comparison of the listing for r in the above table with the requirements on M imposed by Lemma 1 shows that they are consistent except for the last case which needs further consideration. The only possibility of trouble for this case is when none of

$$c_2(f) = (2\alpha, -JM)_2, \qquad c_2(f) = (2\beta, -JM)_2$$

hold for $M \equiv -\alpha_1 J/2$ or $-\beta_1 J/2 \pmod 8$; that is, all of

$$(2\alpha, +2\alpha_1)_2, \quad (2\alpha, +2\beta_1)_2, \quad (2\beta, +2\alpha_1)_2, \quad (2\beta, +2\beta_1)_2$$

are equal to $-c_2(f)$. This is impossible since their product is equal to $(\alpha\beta, \alpha_1\beta_1)_2$ which has the value -1.

Thus we have shown that F represents a prime M_1 or double such a prime consistent with the requirements of Lemma 1. In similar fashion f' may be shown to represent a prime q' congruent to q for an arbitrary modulus. Then F' represents a binary form $-g'$ which represents a prime $-M_2$ congruent to $M_1 \pmod{8K}$ since the determinant of g' has at most a factor of 2 in common with K. Then a prime $M \equiv M_1 \pmod{q}$ and $\equiv M_2 \pmod{q'}$ as well as congruent to $M_1 \pmod{8K}$ will be represented by both F and F'. This completes the proof.

THE UNIVERSITY OF COLORADO.

BIBLIOGRAPHY.

[1] L. E. Dickson, *Studies in the theory of numbers*, University of Chicago Press, 1930.

[2] M. Eichler, *Quadratische Formen und Orthogonale Gruppen*, Berlin, 1952.

[3] B. W. Jones, *The Arithmetic Theory of Quadratic Forms*, New York, 1950.

[4] A. Meyer, *Zur Theorie der unbestimmten ternären quadratischen Formen*, Zürich, 1871.

[5] ———, "Zur Theorie der Indefiniten Ternären Quadratischen Formen," *Journal für Mathematik*, vol. 108 (1891), pp. 125-139.

ON THE BEHAVIOR OF INVARIANT CURVES NEAR A HYPERBOLIC POINT OF A SURFACE TRANSFORMATION.*

By SHLOMO STERNBERG.

1. In [2], Poincaré considered surface transformations of the type

$$x_1 = sx + f(x, y), \qquad y_1 = ty + g(x, y), \tag{1}$$

where s and t are real with $s > 1 > t > 0$, and where f and g are real analytic functions of x and y which vanish at the origin together with their first derivatives. He proved, by the majorant method, that there exist two analytic invariant curves each tangent to one of the axes. In the case of dynamics, the relation $st = 1$ holds (as a necessary condition for the transformation to be area preserving). We shall not make use of this condition. Hadamard [1], treating the case where f and g are merely assumed to be of the class C^1 (and to vanish at the origin along with their first derivatives), showed the existence of invariant curves by the method of successive approximations. In paragraphs 2-6 we shall treat questions of existence and uniqueness of invariant curves by a geometric method under slightly less restrictive conditions and show that our results are, in a sense, the best possible. In paragraphs 7 and 8 we shall deal with questions of smoothness of invariant curves and show that a C^n assumption on the non-linear terms implies that the invariant curves are of class C^n $(n \geqq 1)$. The problems treated in this paper were suggested to the author by Professor Wintner.

2. Let T be a transformation of type (1) which is topological in some neighborhood of the origin. Let $s > 1 > t > 0$, and let the functions f, g be continuous and $o(r)$ as $r = (x^2 + y^2)^{\frac{1}{2}} \to 0$. It is then clear that for all points sufficiently close to the origin, the y coordinate is decreased and the x coordinate is increased upon application of T. Thus if an arc passing through the origin is to be invariant, it must be tangent to one of the axes or else experience oscillations of increasing amplitude and frequency near the origin. In the latter case we shall, naturally, not speak of an "invariant curve." Hence, either the arc is tangent to the x-axis at the origin, in which case all points of the arc move in toward the origin upon application of T; or

* Received February 7, 1955.

the arc is tangent to the y-axis, in which case all the points move away from the origin.

3. In this paragraph and the following, S and T will denote transformations of type (1) where $t > 1$, $t > s$ and $s > 1$, $s > t$ respectively.

THEOREM 1. *Let S be a transformation of type* (1) *where $0 < s < 1$, $s < t$ and where f, g are continuous and are $o(r)$ as $r = (x^2 + y^2)^{\frac{1}{2}} \to 0$. Then there exist a neighborhood N of the origin and a closed set E in N such that* 1) *E is invariant under S,* 2) *for every abscissa x in N there exists a point (x, y) of E,* 3) *E is tangent to the x-axis of the origin* (i.e., given any $\epsilon > 0$, for all sufficiently small $|x|$, all points (x, y) of E lie in the angular region $|y| \leqq \epsilon |x|$).

Proof. We can restrict our attention to the right half plane $x \geqq 0$ since the argument is the same for the left half plane. Consider a point (x, y) on the line $y = \alpha x$, $\alpha > 0$. Its image will be the point (x_1, y_1), where $x_1 = sx + f(x, y)$, $y_1 = ty + g(x, y)$. Thus

$$y_1/x_1 = \{\alpha t/s + g(x, y)/sx\}/\{1 + f(x, y)/sx\}.$$

Since $y = \alpha x$ and both f and g are $o(r)$, we find that $x_1 < x$ and $y_1 > \alpha x_1$ for all sufficiently small positive x, say, for $0 < x \leqq x_0$.

In other words, a point on the line $y = \alpha x$ is moved to the left and above the line by S for all $x < x_0$. Similarly, a point on the line $y = -\alpha x$ is moved to the left and below the line. For all $x < x_0$, let $E^0(x)$ denote the vertical line segment joining the points $(x, -\alpha x)$ and $(x, \alpha x)$. Now S will map $E^0(x)$ into a set containing a connected arc joining a point above the wedge $|y| \leqq \alpha x$ to a point below the wedge. Let $E^1(x)$ denote the subset of $E^0(x)$ consisting of those points whose images under S lie in the wedge $|y| \leqq \alpha x$. If $E^0(x), E^1(x), \cdots, E^{n-1}(x)$ have been defined, let $E^n(x)$ denote the subset of $E^{n-1}(x)$ consisting of those points whose images under S^n lie in the wedge. Since, by induction, the image of $E^{n-1}(x)$ under S^n contains a connected arc joining a point above the wedge to a point below it, $E^n(x)$ is not empty. $E^n(x)$ is clearly closed for all n. Hence $E(x) = \bigcap_n E^n(x)$ is a non-empty closed subset of $E^0(x)$. It is clear that given any ϵ we can find a positive number ξ such that for all $0 < x \leqq \xi$ and all $k \geqq \epsilon$, S takes a point on the line $y = kx$ into a point above the line $y = (k + \tau)x$ where τ is independent of x and k. Hence for a point (x, y) with $x \leqq \xi$ to lie in E we must have $|y| < \epsilon x$. Thus $E(x)$ is tangent to the x-axis at the origin.

Let $E = \bigcup_x E(x)$. Then E is clearly invariant under S. In fact, any subset of the wedge invariant under S is eventually contained in E. Furthermore, a point $P = (x, y)$ of the closed wedge $|y| \leqq \alpha x$, $0 \leqq x \leqq x_0$ is not in E only if S^n, for some positive n, carries P outside the closed wedge. But then a small neighborhood about P is carried outside the wedge by S^n. Thus the complement of E is open, so that E is closed. This proves 1), 2) and 3).

THEOREM 2. *Let T be a transformation of type* (1) *where $s > 1$, $s > t$ and f and g are continuous and $o(r)$ as $r \to 0$. Then there exist a neighborhood N of the origin and a closed set E satisfying* 1), 2), *and* 3) *of Theorem* 1 *where, by invariance, we mean $T(E) \cap N = E$.*

Remark. If T is topological, then Theorem 2 can be obtained by applying Theorem 1 to $S = T^{-1}$.

In order to prove Theorem 2, let us consider an angular wedge W: $|y| \leqq kx$. Then from arguments similar to the above we have

$$(T(W) \cap N) \subset (W \cap N).$$

Let

$$F_0 = W \cap N, \qquad F_1 = T(W \cap N) \cap N$$

and in general $F_n = T(F_{n-1}) \cap N$. It is clear, by induction, that $F_{n+1} \subset F_n$ and thus $E = \bigcap_n F_n$ is a non-empty closed set. It is clear from arguments similar to those of the preceding theorem that 1), 2) and 3) are satisfied.

4. We shall now show that, under the hypotheses of Theorem 1, $E(x)$ can contain more than one point. S will be a transformation of type (1) in which $f \equiv 0$. We shall choose g such that $g(x, 0) = 0$ and so that the x-axis is an invariant curve.

Let $y = \psi(x)$ be a smooth curve tangent to the x-axis at the origin and such that $\psi(x) > 0$ for $x > 0$. In order that $\psi(x)$ be an invariant curve, it is necessary and sufficient that the functional equation

$$t\psi(x) + g(x, \psi(x)) = \psi(sx) \tag{2}$$

be satisfied. Rewriting this we obtain the condition on g

$$g(x, \psi(x)) = \psi(sx) - t\psi(x). \tag{2'}$$

We now define g as follows: Let $g(x, y)$ be 0, $\{\psi(sx) - t\psi(x)\}y/\psi(x)$ or $\psi(sx) - t\psi(x)$ according as $y \leqq 0$, $0 \leqq y \leqq \psi(x)$ or $y \geqq \psi(x)$. We must now verify that the mapping S, with $f \equiv 0$ and g defined as above, satisfies

the conditions of Theorem 1. (It is clear that ψ can be so chosen that the mapping is even topological.) Now $|g(x,y)| \leqq \psi(sx) + t\psi(x)$. Thus g is $o(|x|)$ and so *a fortiori* $o(r)$.

We have constructed g so that (2′) is satisfied; hence, both $y = \psi(x)$ and $y = 0$ are invariant curves of S.

5. We now consider the question of uniqueness.

THEOREM 3. *If the hypotheses of Theorem* 1 *are satisfied, and if both f and g satisfy uniform Lipschitz conditions with respect to x and y, where in a neighborhood of the origin, the uniform Lipschitz constants are less than $\delta < \frac{1}{4}(t-s)$, then, in a suitably small neighborhood N, E is a curve $y = \psi(x)$. In other words, there exists a unique invariant arc in any wedge $|y| \leqq k|x|$ for sufficiently small $|x|$.*

In order to prove this theorem it will suffice to show that given any wedge $|y| \leqq kx$ there exists a positive number ξ such that there cannot be two points (x,y) and (x,y'), where $0 < x \leqq \xi$ and $y > y'$, whose images under S^n are in $|y| \leqq kx$ for all non-negative n.

Since f is $o(r)$, any point in $|y| \leqq kx$ with sufficiently small abscissa $x\,(>0)$ is mapped into a point whose abscissa is smaller than $(s+\epsilon)^n x$. Thus if (x_n, y_n) and (x'_n, y'_n) denote the images under S^n of (x,y), (x,y'), we must have $x_n, x'_n < (s+\epsilon)^n x$ and consequently, $|y_n - y'_n| < 2k(s+\epsilon)^n x$ in order that these images all lie in $|y| \leqq kx$. We shall show that this is impossible for all suitably small x.

From (1), $x_n - x'_n = s(x_{n-1} - x'_{n-1}) + f(x_{n-1}, y_{n-1}) - f(x'_{n-1}, y'_{n-1})$. Thus, for all sufficiently small x,

$$|x_n - x'_n| \leqq s|x_{n-1} - x'_{n-1}| + \delta|x_{n-1} - x'_{n-1}| + \delta|y_{n-1} - y'_{n-1}|.$$

Similarly, $y_n - y'_n = t(y_{n-1} - y'_{n-1}) + g(x_n, y_n) - g(x'_n, y'_n)$; so that

$$|y_n - y'_n| > t|y_{n-1} - y_{n-1}| - \delta|x_{n-1} - x'_{n-1}| - \delta|y_{n-1} - y'_{n-1}|.$$

Now assume that

$$|x_{n-1} - x'_{n-1}| < |y_{n-1} - y'_{n-1}|; \tag{3}$$

then we have

$$|x_n - x'_n| < (s+2\delta)|y_{n-1} - y'_{n-1}| \quad \text{and} \quad |y_n - y'_n| > (t-2\delta)|y_{n-1} - y'_{n-1}|.$$

Since $\delta < \frac{1}{4}(t-s)$ we obtain $|x_n - x'_n| < |y_n - y'_n|$. As $|x_0 - x'_0| = 0 < |y_0 - y'_0|$, the inequality (3) is true for all n, by induction. We thus obtain

$$|y_n - y'_n| > (t-2\delta)|y_{n-1} - y'_{n-1}| \quad \text{or} \quad |y_n - y'_n| > (t-2\delta)^n|y - y'|.$$

We must therefore have $(t-2\delta)^n \mid y-y' \mid < 2k(s+\epsilon)^n x$, which is clearly impossible for all n if ϵ is chosen to be less than $\frac{1}{2}(t-s)$. Thus $y=y'$ and the theorem is established.

6. Let us now consider a transformation T satisfying the hypotheses of Theorem 2. The set E, in virtue of its construction, contains any invariant set lying in the intersection of any angular wedge $\mid y \mid \leqq kx$ and some sufficiently small neighborhood of the origin. Now let G_0 be any set lying entirely in such a region. It follows, from reasoning similar to that of paragraph 3, that the image of this set under T, G_1, still lies in the angular region $\mid y \mid \leqq kx$. Let $G_0, G_1, G_2, \cdots, G_n$ be the sequence of sets so obtained. Let C be the set of limit points of this sequence. C is obviously an invariant set and hence a subset of E. In particular, if E reduces to a curve, then all the successive approximations converge to the invariant curve. Let us now assume that both f and g satisfy uniform Lipschitz conditions (with respect to x and y) where the Lipschitz constant can be made arbitrarily small by restricting ourselves to a small neighborhood of the origin. Let $y=\phi_0(x)$ be a curve satisfying a uniform Lipschitz condition with Lipschitz constant K. Thus $\mid (y-y')/(x-x') \mid < K$. Using the same notation as before, we obtain

$$(y_1-y'_1)/(x_1-x'_1)$$
$$= \{t(y-y')+g(x,y)-g(x',y')\}/\{s(x-x')+f(x,y)-f(x',y')\}.$$

so that $\mid (y_1-y'_1)/(x_1-x'_1) \mid < \{tK+(1+K)\delta\}/\{s-(1+K)\delta\}$, where δ can be made arbitrarily small by choosing x and x' sufficiently small. Thus in a sufficiently small region about the origin, all the image curves satisfy a Lipschitz condition with Lipschitz constants all smaller than K. Hence the sequence is equi-continuous and the convergence is uniform. This is essentially the case considered by Hadamard [1]. We have thus proved

THEOREM 4. *Let T be a transformation of type* (1) *where $s>1$, $s>t$, f and g are continuous and $o(r)$. Furthermore let the set E of Theorem 2 be a curve. Then the sequence of successive images of a set situated in an angular region $\mid y \mid < kx$ converge for sufficiently small x. If, in addition, f and g satisfy uniform Lipschitz conditions with Lipschitz constants which are $o(1)$ as $r \to 0$, then the iterates of any curve $y=\phi(x)$ which satisfies a uniform Lipschitz condition converge uniformly for sufficiently small x to the invariant curve, which then must satisfy a uniform Lipschitz condition.*

7. We shall now consider differentiability of the invariant curve.

THEOREM 5. *Let S be a transformation of type* (1), *where* $0 > s > t$, $s > 1$ *and where f and g are of class C^1 and vanish together with their first derivatives at the origin. Then the unique invariant curve tangent to the x-axis at the origin is of class C^1 for all sufficiently small x.*

In order to make the method clear, we shall first go through the proof for the particular case when $f(x, y) \equiv 0$. Let $y = \psi(x)$ be the invariant curve. It must then satisfy the functional equation (2). Writing this equation for two distinct points x and x' and subtracting, we obtain

$$t\psi(x) - t\psi(x') + g(x, \psi(x)) - g(x', \psi(x')) = \psi(sx) - \psi(sx').$$

Applying the mean value theorem, we obtain

$$t\{\psi(x) - \psi(x')\}/(x - x') + g_x(\xi^*, \psi(x)) + g_y(x', \psi(\xi))\{\psi(x) - \psi(x')\}/(x - x')$$
$$= \{\psi(sx) - \psi(sx')\}/(x - x') \text{ or}$$

$$\{\psi(x) - \psi(x')\}/(x - x')$$
$$= [t + g_y(x', \psi(\xi))]^{-1}[-g_x(\xi^*, \psi(x)) + s\{\psi(sx) - \psi(sx')\}/(sx - sx')],$$

where both ξ and ξ^* lie between x and x'.

We have thus expressed $\{\psi(x) - \psi(x')\}/(x - x')$ in terms of

$$\{\psi(sx) - \psi(sx')\}/(sx - sx').$$

Repeating the process n times, we obtain

$$\{\psi(x) - \psi(x')\}/(x - x')$$
$$= -\sum_{k=1}^{n} s^{k-1} g_x(\xi^*_{k-1}, \psi(s^{k-1}x))\{\prod_{j=1}^{k}(t + g_y(s^{j-1}x, \psi(\xi_{j-1})))\}^{-1}$$
$$+ s^n\{\prod_{j=1}^{n}(t + g_y(s^{j-1}x, \psi(\xi_{j-1})))\}^{-1}\{\psi(s^n x) - \psi(s^n x')\}/(s^n x - s^n x'),$$

where both ξ_j and ξ^*_j lie between $s^j x$ and $s^j x'$.

Now $\psi(x)$ satisfies a uniform Lipschitz condition (by Theorem 4) and $|g_y| < t - s - \delta$ for all sufficiently small x and x'. Thus the second term in the above equation tends to zero and we obtain

$$\{\psi(x) - \psi(x')\}/(x - x') = \sum_{k=1}^{\infty} s^k g_x(\xi^*_{k-1}, \psi(s^{k-1}x)) \prod_{j=1}^{k}(t + g_y(s^{j-1}x, \psi(\xi_{j-1})))^{-1}.$$

Since g_x and g_y are $o(1)$ as $r \to 0$, this series is majorized by a series of the

form $\sum_k s^{k-1}(t-\epsilon)^{-k}$ and so is uniformly convergent. We can, therefore, let $x \to x'$ and obtain

$$\psi'(x) = \sum_{k=1}^{\infty} s^{k-1} g_x(s^{n-1}x, \psi(s^{k-1}x)) \prod_{j=1}^{k} (t + g_y(s^{j-1}x, \psi(s^{j-1}x)))^{-1}.$$

In the case where f is not identically zero the iteration is more difficult. The functional equation satisfied by the invariant curve $\psi(x)$ now takes the form

$$t\psi(x) + g(x, \psi(x)) = \psi(sx + f(x, \psi(x)).$$

(This is the functional equation used by Poincaré [2]). Proceeding as before,

$$t\{\psi(x) - \psi(x')\} + g(x, \psi(x)) - g(x', \psi(x')) = \psi(x_1) - \psi(x'_1),$$

where $(x_1, \psi(x_1))$ and $(x'_1, \psi(x'_1))$ are the images, respectively, of $(x, \psi(x))$ and $(x', \psi(x'))$. Thus

$$\begin{aligned} t\{\psi(x) - \psi(x')\}/(x - x') + g_x(\xi^*, \psi(x)) + g_y(x', \psi(\xi))\{\psi(x) - \psi(x')\}/(x - x') \\ = [\{\psi(x_1) - \psi(x'_1)\}/(x_1 - x'_1)][s + f_x(\eta^*, \psi(x)) \\ + f_y(x', \psi(\eta))\{\psi(x) - \psi(x')\}/(x - x')], \end{aligned}$$

where ξ, ξ^*, η and η^* are all between x and x'. Hence, the iteration takes the form $[\ ]_0 = \{(s + \sigma_0)[\ ]_1 + \delta_0\}\{\epsilon_0[\ ]_1 + (t + \tau_0)\}^{-1}$, where

$$[\ ]_0 = \{\psi(x) - \psi(x')\}/(x - x'), \qquad [\ ]_1 = \{\psi(x_1) - \psi(x'_1)\}/(x_1 - x'_1),$$

$$\sigma_0 = f_x(\eta^*, \psi(x)), \quad \delta_0 = -g_x(\xi^*, \psi(x)), \quad \epsilon_0 = f_y(x', \psi(\eta)), \quad \tau_0 = g_y(x', \psi(\xi)).$$

Introducing corresponding notations for the k-th iterate of this relation, we obtain

$$[\ ]_0 = \prod_{j=0}^{k} \begin{pmatrix} s + \sigma_j & \delta_j \\ \epsilon_j & t + \tau_j \end{pmatrix} [\ ]_{k+1}, \text{ where } \begin{pmatrix} a & b \\ c & d \end{pmatrix}(z) = (az + b)/(cz + d),$$

and the product denotes matrix multiplication.

We now wish to establish the convergence of this iteration. We first show that for all sufficiently small x and x', the product

$$\prod_{j=0}^{k} \begin{pmatrix} s + \sigma_j & \delta_j \\ \epsilon_j & t + \tau_j \end{pmatrix}$$

can be put in the form

$$\begin{pmatrix} A_k & B_k \\ C_k & 1 + D_k \end{pmatrix}, \text{ where } A_k = A \prod_1^k \alpha_j, C_k = C \prod_1^k \gamma_j,$$

with $|\alpha_j| < r < 1$, $|\gamma_j| < r < 1$, and $B_k = B_{k-1} + \beta_k$, $D_k = D_{k-1} + \vartheta_k$, with

$|\beta_k| < p^k$, $|\partial_k| < p^k$, and $|p| < 1$. This is certainly true for the case $k = 0$. We shall prove that the matrix has this form for all n, by induction. Thus assume the proposition true for the case $k = n$. Then the $(n+1)$-st matrix is

$$\begin{pmatrix} A_n & B_n \\ C_n & 1+D_n \end{pmatrix}\begin{pmatrix} s+\sigma_n & \delta_n \\ \epsilon_n & t+\tau_n \end{pmatrix}.$$

Now since this matrix product is considered as acting as a linear fractional transformation we may divide all four elements by the same amount without changing the effect of the matrix. Carrying out the matrix multiplication and dividing by $t+\tau_n$ we obtain the matrix

$$\begin{pmatrix} A_n(s+\sigma_n)\rho_n + B_n\epsilon_n\rho_n & A_n\delta_n\rho_n + B_n \\ C_n(s+\sigma_n)\rho_n + (1+D_n)\epsilon_n\rho_n & 1+D_n+C_n\delta_n\rho_n \end{pmatrix},$$

where $\rho_n = 1/(t+\tau_n)$. Now by virtue of the inductive hypothesis, $|B_n| < B$ and $|D_n| < D$, where B and D do not depend on n. Since σ_n, δ_n, ϵ_n, τ_n are all uniformly $o(1)$ (as x and x' go to zero), we may choose x and x' so small that

$$|(s+\sigma_n+\epsilon_n B/A)/(t+\tau_n)| < r < 1,$$

$$|(s+\sigma_n+\epsilon_n(1+D_n)/C)/(t+\tau_n)| < r < 1,$$

$$|A\delta_n/(t+\tau_n)| < p < 1, \qquad |C\delta_n/(t+\tau_n)| < p < 1.$$

Thus the $(n+1)$-st matrix has the desired form. It should be remarked at this point that the constants C and D are still at our disposal.

As before, we know that the $[\ ]_n$ are uniformly bounded. We now choose C and D so small that the denominator of the n-th iterate never vanishes and the uniform convergence of the iteration process is established.

COROLLARY. *If, in addition to the hypotheses of Theorem* 5, f *and* g *are assumed to be of class* C^u, *then* ψ *is of class* C^n *in some neighborhood of the origin.*

Proof. The function $\psi'(x)$ can be represented as the quotient of two series both of which are majorized by $\sum Kr^n$ with $r < 1$. In taking successive difference quotients, one obtains series majorized by $K\sum M^k(n!/(n-k)!)r^n$, which is also uniformly convergent.

8. Let T be a transformation of type (1), where f and g are of class C^n $(n \geqq 1)$ and vanish at the origin together with their first derivatives. Furthermore, let $s > 1 > t > 0$. Then both T and T^{-1} satisfy the conditions of the corollary to Theorem 5 and hence, there exist exactly two invariant

curves of the transformation T, each tangent to one of the axes at the origin. We can perform a rotation of the coordinate system so that now neither invariant curve touches an axis. In these new (u, v) coordinates the two invariant curves may be represented as $v = \phi_1(u)$ and $v = \phi_2(u)$. We now write $X = v - \phi_1(u)$, $Y = v - \phi_2(u)$. Since the curves ϕ_1 and ϕ_2 are perpendicular at the origin, the Jacobian of this transformation does not vanish. The transformation T is therefore defined in these new variables. We thus have

THEOREM 6. *Let T be a transformation of type* (1) *with $s > 1 > t > 0$. Furthermore, let f and g be of class C^n $(n \geqq 1)$ and vanish at the origin together with their first derivatives. Then there exists a non-singular change of coordinates $X = X(x, y)$, $Y = Y(x, y)$ of class C^n so that in the new coordinates the axes are the invariant curves and T has the form*

$$X_1 = s(X + F(X, Y)), \qquad Y_1 = t(Y + G(X, Y)),$$

where F and G are both of class C^n, and where

$$F(0, y) = G(x, 0) = F_x(0, 0) = F_y(0, 0) = G_x(0, 0) = G_y(0, 0) = 0.$$

THE JOHNS HOPKINS UNIVERSITY.

REFERENCES.

[1] J. Hadamard, *Selecta*, 1901, pp. 163-166.

[2] H. Poincaré, Œuvres, vol. 1 (1886), pp. 202 204.

ON A PROBLEM OF LITTLEWOOD.*

By R. SALEM.

In his "Research Problems" Littlewood raises the question to know whether it is true that, given n distinct integers $m_1, m_2, \cdots, m_n$, there exists an absolute constant A satisfying

$$\int_0^{2\pi} | e^{m_1 ix} + \cdots + e^{m_n ix} | \, dx > A \log n.$$

The purpose of this paper is to prove the following weaker result.

THEOREM. *Let m_n, $n = 1, 2, \cdots$, be an increasing sequence of positive integers such that $\log m_n = O(\log n)$. Then, as $n \to \infty$,*

$$\limsup \int_0^{2\pi} | \cos m_1 x + \cdots + \cos m_n x | \, dx/(\log n)^{\frac{1}{2}} > 0.$$

The proof is extremely indirect and is based on the refinement of an argument used by the author (see Salem [2]) to give a new proof of the theorem of Menchoff on the convergence almost everywhere of series of orthogonal functions: namely, if $\{\phi_j\}_1^\infty$ is any orthonormal system, and if $\sum \gamma_j^2 \log^2 j < \infty$, then $\sum \gamma_j \phi_j$ converges almost everywhere.

LEMMA I. *Given $\Omega(n)$ increasing to ∞ and such that $\Omega(n) = o(\log^2 n)$, there exists an orthonormal system $\{\phi_j\}_1^\infty$ in $(0, 1)$ and a sequence of coefficients $\{\alpha_j\}_1^\infty$ such that $\sum \alpha_j^2 \Omega(j) < \infty$ and that the series $\sum \alpha_j \phi_j$ diverges almost everywhere.*

This lemma which is equivalent to the rough statement that "Menchoff's theorem can not be improved" is known. (See Kaczmarz and Steinhaus [1].)

LEMMA II. *Given $\Omega(n)$ increasing to ∞ and such that $\Omega(n) = o(\log^2 n)$, there exist*

1) *a fixed orthonormal system $\{\phi_j\}_1^\infty$ in $(0, 1)$,*

2) *for each n, a non-increasing sequence $\{F_j\}_1^n$ of characteristic functions of sets in $(0, 1)$ (depending on n),*

---

* Received December 27, 1954.

3) *for each* n, *a function* $Q \in L^2$ *in* $(0,1)$ *(depending on* n*), with* $\int_0^1 Q^2 dx = 1$, *such that*

$$\limsup \sum_1^n \left(\int_0^1 QF_j\phi_j\,dx\right)^2/\Omega(n) = \infty.$$

Proof. Take for $\{\phi_j\}_1^\infty$ the orthonormal system whose existence is asserted by Lemma I. If it were true that

$$\sum_1^n \left(\int_0^1 QF_j\phi_j\,dx\right)^2 < C\Omega(n), \tag{1}$$

C being a constant, no matter how the sequence $\{F_j\}_1^n$ and the function Q were chosen for each n, it would follow, by a known argument (see Salem [2]) that given any n numbers $\gamma_1, \cdots, \gamma_n$ and writing $S_p(x) = \sum_1^p \gamma_j\phi_j$, one would have

$$\int_0^1 \sup_{1\leqq p\leqq n} |S_p(x)|^2\,dx < C\left(\sum_1^n \gamma_j\right)^2\Omega(n).$$

By the classical argument of Menchoff,[1] this would imply that the series $\sum \alpha_j\phi_j$ converges almost everywhere whenever $\sum \alpha_j^2\Omega(j) < \infty$. Hence, by the particular choice of the system $\{\phi_j\}$, a contradiction to Lemma I.

We shall now prove a third lemma, in which we shall adopt the following notations:

$\{\theta_k(t)\}_1^\infty$ is any orthonormal, uniformly bounded system in $(0,1)$, say $|\theta_k(t)| \leqq M$.

$\{c_k\}_1^\infty$ is any sequence of coefficients, and $s_m(t) = \sum_1^m c_k\theta_k(t)$.

$\{m_j\}_1^\infty$ is any increasing sequence of positive integers.

$\psi(t)$ is of the class L in $(0,1)$, and $\psi(t) \geqq 1$ (ψ may depend on n),

$\{\phi_j(x)\}_1^\infty$ is any orthonormal system in $(0,1)$.

$\{F_j(x)\}_1^n$ is any non-increasing sequence of characteristic functions of sets in $(0,1)$ (which may depend on n).

---

[1] We mean the argument of Menchoff's theorem used to prove that for all orthonormal systems $\{\phi_j\}_1^\infty$, $\int_0^1 \sup_{1\leqq p\leqq n} |S_p(x)|^2 dx < C\left(\sum_1^n \gamma_j^2\right)\log^2 n$ and deducing from this inequality that $\sum \gamma_j\phi_j$ converges almost everywhere whenever $\sum \gamma_j^2 \log^2 j < \infty$.

In order to apply this argument (see, e.g., Kaczmarz and Steinhaus [1]) it is neecssary to suppose that $\Omega(n)/\log n$ exceeds a constant. But this is irrelevant for the proof of Lemma II, since clearly we can replace, in (1), $\Omega(n)$ by a function increasing more rapidly.

$Q(x)$ is any function of the class L^2 in $(0,1)$ (which may depend on n), with $\int_0^1 Q^2(x)\,dx = 1$.

For the sake of simplicity, everything is real.

LEMMA III. *We have, with the preceding notations,*

$$\sum_{j=1}^{n} \left(\int_0^1 QF_j\phi_j\,dx\right)^2 c_{m_j}{}^2 \leqq M^2 \left(\int_0^1 \psi\,dt\right) \cdot \max_{1\leqq j\leqq n} \int_0^1 s_{m_j}(t)/\psi(t)\,dt.$$

Proof. The system of functions $p_j(x,t) = \phi_j(x)\theta_{m_j}(t)\psi(t)^{\frac{1}{2}}$ is orthogonal in the square $0 \leqq t \leqq 1$, $0 \leqq x \leqq 1$. Let

$$(2) \qquad a_j = \int_0^1\int_0^1 p_j^2(x,t)\,dxdt = \int_0^1 \theta_{m_j}{}^2(t)\psi(t)\,dt \leqq M^2 \int_0^1 \psi(t)\,dt,$$

and consider the function

$$P(x,t) = \sum_{k=1}^{m_n} c_k Q(x) f_k(x)\theta_k(t)/\psi(t)^{\frac{1}{2}},$$

where the $\{f_k(x)\}_1{}^{m_n}$ is a non-increasing sequence of m_n characteristic functions of sets in $(0,1)$ which will be determined in a moment.

One has, if $j \leqq n$, $\int_0^1\int_0^1 P(x,t)p_j(x,t)\,dxdt = c_{m_j}\int_0^1 Qf_{m_j}\phi_j dx$, while the left-hand side vanishes if $j > n$. Hence Bessel's inequality gives

$$(3) \qquad \sum_{j=1}^{n} \left(\int_0^1 Qf_{m_j}\phi_j dx\right)^2 c_{m_j}{}^2/a_j \leqq \int_0^1\int_0^1 P^2(x,t)\,dxdt.$$

Now

$$P(x,t) = Q(x)/(\psi(t))^{\frac{1}{2}} \sum_{k=1}^{m_n} f_k(x)c_k\theta_k(t) = Q(x)/(\psi(t))^{\frac{1}{2}} \sum_{1}^{m_n} \Delta f_k \cdot s_k(t),$$

where $\Delta f_k = f_k(x) - f_{k+1}(x)$, $\Delta f_{m_n} = f_{m_n}$. Remembering the definition of $f_k(x)$, we have $P^2(x,t) = Q^2/\psi \sum_{1}^{m_n} \Delta f_k \cdot s_k{}^2(t)$ and

$$\int_0^1\int_0^1 P^2(x,t)\,dxdt = \sum_{1}^{m_n} \left(\int_0^1 Q^2\Delta f_k dx\right)\left(\int_0^1 s_k{}^2(t)/\psi(t)dt\right).$$

Take now

$$f_k = F_j \text{ for } m_{j-1} < k \leqq m_j \qquad (j = 1, 2, \cdots, n),\ (m_0 = 0),$$

and write $\Delta F_j = F_j - F_{j+1}$, $\Delta F_n = F_n$. Then

$$\int_0^1\int_0^1 P^2(x,t)\,dxdt = \sum_{1}^{n} \left(\int_0^1 Q^2\Delta F_j dx\right)\left(\int_0^1 s_{m_j}{}^2(t)/\psi(t)\,dt\right)$$

$$\leqq \max_{1\leqq j\leqq n} \int_0^1 s_{m_j}{}^2(t)/\psi(t)\,dt,$$

since $\int_0^1 Q^2 dx = 1$. Hence, by (3) and (2),

$$\sum_{j=1}^{n} \left(\int_0^1 QF_j\phi_j dx\right)^2 c_{m_j}{}^2 \leqq M^2 \left(\int_0^1 \psi dt\right) \max_{1\leqq j\leqq n} \int_0^1 s_{m_j}{}^2(t)/\psi(t)\, dt,$$

which proves the Lemma.

Proof of the theorem. The notations being the same as in the Lemma, take $\theta_k(t) = \cos(kt - \alpha_k)$, so that the series $\sum c_k\theta_k(t)$ becomes a trigonometric series (the fact that the interval of orthogonality is $(0, 2\pi)$ and that the system is not normalized is obviously irrelevant). We define now:

$$\psi(t) = \psi_n(t) = \sup_{1\leqq j\leqq n} |\, s_{m_j}(t)| + 1,$$

and we suppose that $|\, c_{m_j}| \geqq \delta > 0$. The lemma then gives, A being an absolute constant:

$$\sum_{j=1}^{n} \left(\int_0^1 QF_j\phi_j dx\right)^2 \leqq A/\delta^2 \left(\int_0^{2\pi} \psi_n(t)\, dt\right) \max_{1\leqq j\leqq n} \int_0^{2\pi} |\, s_{m_j}(t)|\, dt.$$

Now it is easily seen, since s_{m_j} is a partial sum of the polynomial s_{m_n}, that

$$\int_0^{2\pi} \psi_n(t)\, dt \leqq C \log m_n \int_0^{2\pi} |\, s_{m_n}(t)|\, dt. \tag{4}$$

Hence

$$\sum_{j=1}^{n} \left(\int_0^1 QF_j\phi_j dx\right)^2 \leqq AC/\delta^2 \log m_n \cdot \max_{1\leqq j\leqq n} \left\{\int_0^{2\pi} |\, s_{m_j}(t)|\, dt\right\}^2.$$

Now suppose that $\log m_n = O(\log n)$. Then the second member of the last inequality is

$$O(\log n) \cdot \max_{1\leqq j\leqq n} \left\{\int_0^{2\pi} |\, s_{m_j}(t)|\, dt\right\}^2.$$

If we had $\lim \int_0^{2\pi} |\, s_{m_j}(t)|\, dt/(\log j)^{\frac{1}{2}} = 0$, the inequality would give

$$\sum_{j=1}^{n} \left(\int_0^1 QF_j\phi_j dx\right)^2 = o(\log^2 n),$$

the second member being independent of $\{\phi_j\}_1{}^\infty$, $\{F_j\}_1{}^n$ and Q. This is impossible, by Lemma II. Hence, if in the series $\sum_1^\infty c_k \cos(kt - \alpha_k)$, whose

m-th partial sum we denote by s_m, we have $|c_{m_j}| \geqq \delta > 0$, $\log m_j = O(\log j)$, then

$$\limsup \int_0^{2\pi} |s_{m_j}(t)|\, dt/(\log j)^{\frac{1}{2}} > 0. \tag{5}$$

This result includes obviously our theorem, which is thus proved.

Remark. Let us observe that if $\sum c_k \cos(kt - \alpha_k)$ is a Fourier-Stieltjes series, one gets a stronger result than (5): for then (4) can be replaced by $\int_0^{2\pi} \psi_n(t)\, dt \leqq B \log m_n$, B being a constant. We have then with the same hypothesis

$$\sum_{j=1}^{n} \left(\int_0^1 QF_j\phi_j dx\right)^2 = O(\log n) \max \int_0^{2\pi} |s_{m_j}(t)|\, dt,$$

which leads, instead of (5) to

$$\limsup \int_0^{2\pi} |s_{m_j}(t)|\, dt/\log j > 0. \tag{6}$$

This is, in particular, the case, if $\liminf \int_0^1 |s_m(t)|\, dt = O(1)$, since this relation implies that $\sum c_k \cos(kt - \alpha_k)$ is a Fourier-Stieltjes series.

Other consequences of Lemma III. Lemma III can be used to prove other results. We shall give one example, which generalizes a result obtained earlier (see Salem [2]).

By $\theta_k(t)$ we denote now generally, as in the Lemma, any orthonormal, uniformly bounded system in $(0, 1)$, with $|\theta_k(t)| \leqq M$. Writing as before $s_m = \sum_1^m c_k\theta_k$, we shall prove that if $|c_{m_j}| \log j \to \infty$ then $\sup_j |s_{m_j}(t)|$ cannot belong to L.

In fact, suppose $\sup_j |s_{m_j}(t)| \in L$, and choose, in the inequality of Lemma III, $\psi(t) = \sup_j |s_{m_j}(t)| + 1$. The inequality becomes

$$\sum_{j=1}^{n} \left(\int_0^1 QF_j\phi_j dx\right)^2 c_{m_j}{}^2 \leqq M^2 \left\{\int_0^1 \psi(t)\, dt\right\}^2.$$

Now, if $|c_{m_j}| \log j \to \infty$, we can find a function $\omega(j) \to \infty$ such that $\omega(j)/\log j$ decreases and that $|c_{m_j}| \log j > \omega(j)$. Hence

$$(\omega(n)/\log n)^2 \sum_{j=1}^{n} \left(\int_0^1 QF_j\phi_j dx\right)^2 \leqq M^2 \left(\int_0^1 \psi dt\right)^2,$$

which again contradicts Lemma II, by a suitable choice of $\{\phi_j\}_1^\infty$, $\{F_j\}_1^n$ and Q.

Hence $\sup_j |s_{m_j}(t)| \varepsilon L$ implies $\liminf |c_{m_j}| \log j = O(1)$.

One deduces immediately (by considering a subsequence of $\{m_j\}$) that $\sup_j |s_{m_j}(t)| \varepsilon L$ implies $c_{m_j} \to 0$.

In particular, $\sup_m |s_m(t)| \varepsilon L$ implies $c_m \to 0$ for any orthonormal, uniformly bounded system. Direct proofs can be given of this result, a remark which I owe to A. Zygmund.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY.

BIBLIOGRAPHY.

[1] S. Kaczmarz and H. Steinhaus, *Orthogonalreihen*, Warszawa-Lwów, 1935.

[2] R. Salem, "A new proof of a theorem of Menchoff," *Duke Mathematical Journal*, vol. 8 (1941), pp. 269-272.

SOME LINEAR MINIMAX PROBLEMS OVER AN ORDERED FIELD.*

By R. J. LEVIT.

1. Introduction. Let S be a subset of an n-dimensional vector space over an ordered field F fixed throughout the paper. If, as the vector $X=(X_1, \cdots, X_n)$ ranges over S, $\max_j |X_j|$ has a minimum value M^*, then M^* is called the *minimax of* S. Clearly, when M^* exists, it may be characterized as the unique element of F satisfying the two conditions,

$$\begin{aligned} &\text{For every } X \varepsilon S \ \max_{j=1,\cdots,n} |X_j| \geqq M^*. \\ &\text{There is a vector } X^* \varepsilon S \text{ such that } \max_{j=1,\cdots,n} |X^*_j| = M^*. \end{aligned} \tag{1.1}$$

A vector X^* satisfying the second of these conditions is called a *minimax vector of* S. It may be regarded as least among the vectors of S in the sense that each component is at least as small in absolute value as some component of every other vector in S.

Given a consistent system of linear equations with coefficients in F,

$$\sum_{j=1}^{n} a_{ij}x_j = a_{i0} \qquad (i=1,\cdots,m), \tag{1.2}$$

let G be a set of integers $g_1, \cdots, g_s$, $1 \leqq g_\nu \leqq n$, and denote by S^G the totality of vectors $(X_{g_1}, \cdots, X_{g_s})$ such that $x=(X_1, \cdots, X_n)$ is a solution of (1.2). The minimax M^G of S^G we call the *minimax of the system with respect to* $x_{g_1}, \cdots, x_{g_s}$. Thus, M^G is the minimum value of $\max_{j \varepsilon G} |X_j|$ as X ranges over all solutions of (1.2). A minimax vector X^G of S^G we call a *minimax solution with respect to* $x_{g_1}, \cdots, x_{g_s}$. Our main result is the determination of M^G and the characterization of the minimax solutions with respect to $x_{g_1}, \cdots, x_{g_s}$ for the system (1.2). If certain submatrices of the matrix of (1.2) are non-singular, there is a unique minimax solution X^G, and an explicit formula is given for it. These results are obtained in Section 4 utilizing the already known case of a single equation [1], which is discussed in Section 2, and the notion of a Plücker array, which is defined and developed in Section 3.

* Received July 7, 1953; revised December 15, 1954.

In Section 5 the results of Section 4 are applied to determine the minimax M^* of the range of a vector function $L(x_1, \cdots, x_q)$ having as components the linear functions,[1]

$$L_i(x_1, \cdots, x_q) = \sum_{j=1}^{q} b_{ij}x_j - b_{i0} \qquad (i = 1, \cdots, n), \tag{1.3}$$

as $x_1, \cdots, x_q$ range independently over F. In this case M^* is called *the minimax of the system of linear functions.* The vectors $X^* = (X^*_1, \cdots, X^*_q)$ such that $\max_i |L_i(X^*)| = M^*$, called *the minimax points of the system,* are characterized also.

In Section 6 the results of Section 4 and Section 5 are applied to some problems of best approximation in the Tchebycheff sense; namely determination of best approximate solutions to inconsistent systems of linear equations[2] and best approximation of arbitrary function on finite sets. The latter generalizes some results of De La Vallée Poussin [5].

2. The minimax solutions of a single equation. We consider the equation,

$$\sum_{j=1}^{n} a_j x_j = a_0 \qquad (a_j \varepsilon F). \tag{2.1}$$

LEMMA 1.1. *If X is a solution of (2.1) and $a_j \neq 0$ for at least one integer j, $1 \leqq j \leqq n$, then $\max_{j=1,\cdots,n} |X_j| \geqq |\mu|$, where*

$$\mu = a_0 / \sum_{j=1}^{n} |a_j|. \tag{2.2}$$

Proof. The result follows immediately from

$$|a_0| \leqq \sum_{j=1}^{n} |a_j|\,|X_j| \leqq (\max |X_j|) \sum_{j=1}^{n} |a_j|. \tag{2.3}$$

THEOREM 1. *Denote the set $\{1, \cdots, n\}$ by N. If in (2.1) $a_j \neq 0$ for at least one $j \varepsilon N$, the solutions have the minimax $M^N = |\mu|$. Let D be the set of integers $j \varepsilon N$ for which $a_j = 0$. Then X^N is a minimax solution if and only if*

$$|X^N{}_j| \leqq |\mu| \ (j \varepsilon D); \qquad X^N{}_j = \mu \operatorname{sgn} a_j \quad (j \varepsilon N - D). \tag{2.4}$$

[1] This problem has been solved in the field of real numbers by M. Krein [3] using functional analysis and in the field of complex numbers by V. K. Ivanov [2].

[2] This problem has recently been treated in the field of complex numbers by E. Remez [4].

Proof. Consider first the case $a_0 a_1 \cdot \cdot \cdot a_n \neq 0$. By the lemma $|\mu|$ satisfies the first minimax condition (1.1). For a solution X of (2.1) equality holds between the first and second members of (2.3) if and only if the non-vanishing terms in the sum $\sum a_j X_j$ all have the same sign (which is then necessarily the sign of a_0) and between the second and third members if and only if the X_j all have the same absolute value. Hence, $\max |X_j| = |\mu|$ if and only if $\operatorname{sgn} X_j = \operatorname{sgn} a_0 a_j = \operatorname{sgn} \mu a_j$ and $|X_j| = |\mu|$ for $j = 1, \cdot \cdot \cdot, n$. Since direct substitution with the aid of (2.2) verifies that $x_j = \mu \operatorname{sgn} a_j$ is a solution of (2.1), $|\mu|$ also satisfies the second minimax condition (1.1) with the second expression (2.4) as the minimax solution, which is unique in this case. The proof for D empty is then completed by noting that, when $a_0 = 0$, the unique minimax solution is $X^N{}_j = 0$, $j = 1, \cdot \cdot \cdot, n$. Finally, when D is not empty, we apply the foregoing result to the system $\sum_{j \varepsilon N-D} a_j x_j = a_0$. Then, since $a_0 / \sum_{j \varepsilon N-D} |a_j| = \mu$, the theorem is proved.

3. Sign-compatibility of Plücker arrays. Any skew-symmetric square array over F of rank two or less we call a *Plücker array* (P. a.). The existence proof for minimax solutions of (1.1) depends on the property of these arrays stated in Theorem 2 below, which involves the following notion. Two vectors,

$$C_1 = (c_{11}, \cdot \cdot \cdot, c_{1s}), \qquad C_2 = (c_{21}, \cdot \cdot \cdot, c_{2s}), \tag{3.1}$$

over F are called *sign-compatible* (s. c.) if $\operatorname{sgn} c_{1j} c_{2j} c_{1k} c_{2k} \neq -1$ for $j, k = 1, \cdot \cdot \cdot, s$. This relation is evidently symmetric and reflexive but is not transitive; e. g., of the vectors $(1, 1, 1)$, $(1, 0, 1)$, $(1, -1, 1)$ the first and second are s. c. as are the second and third but not the first and third.

LEMMA 2.1. *Let the vectors* (3.1) *contain a pair of corresponding components* c_{1a} *and* c_{2a} *such that* $c_{1a} c_{2a} \neq 0$. *Then* C_1 *and* C_2 *are s. c. if and only if*

$$\operatorname{sgn} c_{1j} c_{2j} = \operatorname{sgn} c_{1a} c_{2a} \tag{3.2}$$

whenever $c_{1j} c_{2j} \neq 0$.

Proof. If C_1 and C_2 are s. c. and $c_{1j} c_{2j} \neq 0$, $\operatorname{sgn} c_{1j} c_{2j} c_{1a} c_{2a} = 1$, and (3.2) follows. Conversely, assume (3.2) holds whenever $c_{1j} c_{2j} \neq 0$. Then for arbitrary $j, k = 1, \cdot \cdot \cdot, s$ either $c_{1j} c_{2j} c_{1k} c_{2k} = 0$ or

$$\operatorname{sgn} c_{1j} c_{2j} = \operatorname{sgn} c_{1a} c_{2a} = \operatorname{sgn} c_{1k} c_{2k} \neq 0$$

so that $\operatorname{sgn} c_{1j} c_{2j} c_{1k} c_{2k} = 1$. Hence, C_1 and C_2 are s. c.

LEMMA 2.2. *If vectors C_p, C_q, C_r are rows of a P.a. $C = (c_{ij})$, then*

$$c_{qr}C_p + c_{rp}C_q + c_{pq}C_r = 0. \tag{3.3}$$

Proof. If

$$c_{pq} = c_{qr} = c_{rp} = 0, \tag{3.4}$$

(3.3) holds trivially; hence, we assume (3.4) does not hold. Since the rank of C is not more than two, there are elements k_1, k_2, $k_3 \varepsilon F$ not all zero such that

$$k_1c_{pj} + k_2c_{qj} + k_3c_{rj} = 0, \qquad (j = 1, \cdots, s) \tag{3.5}$$

where s is the order of C. For definiteness we assume $k_3 \neq 0$. Then, writing (3.5) in the cases $j = p$ and $j = q$ and applying the skew-symmetry of C, we obtain respectively

$$-k_2c_{pq} + k_3c_{rp} = 0, \qquad k_1c_{pq} - k_3c_{qr} = 0.$$

These imply that $c_{pq} \neq 0$, since otherwise (3.4) would hold. Hence, $k_2 = k_3c_{rp}/c_{pq}$, $k_1 = k_3c_{qr}/c_{pq}$. Substituting these values into (3.5), we obtain (3.3).

LEMMA 2.3. *Two rows C_p and C_q of a P.a. $C = (c_{ij})$ are proportional if and only if $c_{pq} = 0$.*

Proof. Let $c_{pj} = kc_{qj}$, $j = 1, \cdots, s$, where s is the order of C and $k \varepsilon F$. Then in particular, $c_{pq} = kc_{qq} = 0$, since C is skew-symmetric. Conversely, let $c_{pq} = 0$. If $c_{pj} = 0$ for $j = 1, \cdots, s$, C_p and C_q are proportional. Otherwise, there is an element $c_{pr} \neq 0$; so $c_{rp} = -c_{pr} \neq 0$. By Lemma 2.2 $c_{qr}C_p + c_{rp}C_q = 0$. Hence, C_p and C_q are proportional.

A P.a. is said to be reducible if two of its rows are proportional. By the lemma just proved a P.a. is irreducible (not reducible) if and only if all its zero elements lie in the main diagonal. Let $C = (c_{ij})$ be a reducible P.a. of order s with row C_b proportional to C_a.

$$c_{bj} = kc_{aj} \qquad (j = 1, \cdots, s; k \varepsilon F). \tag{3.6}$$

The sub-array C' obtained from C by deleting the row and column of index b is called a *direct reduction of* C. An $(s-n)$-rowed minor array $C^{(n)}$ of C is called a *reduction of* C if there is a sequence $C', C'', \cdots, C^{(n-1)}$ of reducible sub-arrays of C each of which is a direct reduction of its immediate predecessor and such that C' is a direct reduction of C and $C^{(n)}$ of $C^{(n-1)}$. It is convenient to regard $C^{(0)} = C$ as itself a reduction of C. Clearly, a reduction of a P.a.

is again a P.a. We use the symbol $C^{(n)}{}_i$ to denote the row $(c_{ij_1}, \cdots, c_{ij_{s-n}})$ of $C^{(n)}$.

LEMMA 2.4. *Two rows $C^{(n)}{}_d$ and $C^{(n)}{}_e$ in a reduction $C^{(n)}$ of a reducible P.a. $C = (c_{ij})$ are proportional if and only if C_d and C_e are proportional and are s.c. if and only if C_d and C_e are s.c.*

Proof. It is sufficient to prove the lemma for $n = 1$; i.e., for a direct reduction C' of C. Let C'_d and C'_e be proportional. Then by Lemma 2.3 $c_{de} = 0$, and hence, C_d and C_e are proportional. Next, let C'_d and C'_e be s.c., and suppose that C' has been obtained from C by deleting the row and column of index b so that (3.6) holds for some integer a. Then,

$$\operatorname{sgn} c_{dj}c_{ej}c_{dm}c_{em} \neq -1 \tag{3.7}$$

holds for every $j, m = 1, \cdots, b-1, b+1, \cdots, s$. But

$$\operatorname{sgn} c_{dj}c_{ej}c_{db}c_{eb} = \operatorname{sgn} c_{dj}c_{ej}c_{bd}c_{be} = \operatorname{sgn} c_{dj}c_{ej}k^2c_{ad}c_{ae} = \operatorname{sgn} k^2c_{dj}c_{ej}c_{da}c_{ea} \neq -1$$

by (3.6), (3.7). That is, (3.7) holds for $m = b$ also so that C_d and C_e are s.c. The converses are trivial.

LEMMA 2.5. *If a P.a. $C = (c_{ij})$ contains a set of r rows no two of which are proportional, so does any reduction of C.*

Proof. It is sufficient to prove the lemma for a direct reduction C'. Let C' be obtained from C by deleting the row and column of index b so that (3.6) holds for some a. Let I be the set of indices of the r rows in question. If $b \notin I$, the conclusion is an immediate consequence of the preceding lemma. Otherwise, $a \notin I$ and the set $\{C'_i\}$ for $i \in I - \{b\} + \{a\}$ is composed of r rows of C'. By Lemma 2.4 no two of these rows are proportional except possibly C'_a and some row C'_d with $d \in I - \{b\}$. But, since C_b and C_d are not proportional, $c_{bd} \neq 0$ by Lemma 2.3. Hence, $c_{ad} \neq 0$ by (3.6), and accordingly by Lemma 2.3 C'_a and C'_d are not proportional either.

LEMMA 2.6. *Let (c_{ij}) be an irreducible P.a. of order $s \geqq 4$; define the vectors $V_{in} = (c_{i1}, c_{i2}, \cdots, c_{in})$, $n = 1, \cdots, s$, and let d, e, m be integers, $d \neq e$, $1 < d \leqq m < s$, $1 < e \leqq m$. Then if V_{1m} is s.c. with both V_{dm} and V_{em}, $V_{1,m+1}$ is s.c. with at least two of the vectors, $V_{d,m+1}$, $V_{e,m+1}$, $V_{m+1,m+1}$.*

Proof. If $V_{d,m+1}$ and $V_{e,m+1}$ are both s.c. with $V_{1,m+1}$, there is nothing to prove. Otherwise, we assume without loss of generality that $V_{d,m+1}$ is not s.c. with $V_{1,m+1}$. Then there is an integer a, $1 < a \leqq m$, such that $\operatorname{sgn} c_{1a}c_{da}c_{1,m+1}c_{d,m+1} = -1$, or $\operatorname{sgn} c_{1a}c_{da} = -\operatorname{sgn} c_{1,m+1}c_{d,m+1} \neq 0$. But, by

Lemma 2.1 for every integer $j \neq d$ such that $1 < j \leqq m$, $\operatorname{sgn} c_{1j}c_{dj} = \operatorname{sgn} c_{1a}c_{da}$, since $c_{lj} \neq 0$ for $j \neq i$ by Lemma 2.3. Hence,

$$\operatorname{sgn} c_{1j}c_{dj} = -\operatorname{sgn} c_{1,m+1}c_{d,m+1} \neq 0 \qquad (1 < j \leqq m, j \neq d), \tag{3.8}$$

and in particular $\operatorname{sgn} c_{1e}c_{de} = -\operatorname{sgn} c_{1,m+1}c_{d,m+1} \neq 0$, so that because of the skew-symmetry

$$\operatorname{sgn} c_{de}c_{1,m+1} = \operatorname{sgn} c_{e1}c_{d,m+1} \neq 0. \tag{3.9}$$

Similarly, if $V_{e,m+1}$ were not s.c. with $V_{1,m+1}$, $\operatorname{sgn} c_{ed}c_{1,m+1} = \operatorname{sgn} c_{d1}c_{e,m+1} \neq 0$, or $\operatorname{sgn} c_{de}c_{1,m+1} = \operatorname{sgn} c_{1d}c_{e,m+1} \neq 0$. This combined with (3.9) would imply that $c_{de}c_{1,m+1} + c_{e1}c_{d,m+1} + c_{1d}c_{e,m+1} \neq 0$ contrary to Lemma 2.2. Hence, $V_{e,m+1}$ is s.c. with $V_{1,m+1}$. Since by Lemma 2.2 $c_{m+1,1}c_{jd} + c_{1j}c_{m+1,d} + c_{j,m+1}c_{1d} = 0$ and, for $j \neq d$ such that $1 < j \leqq m$, $\operatorname{sgn} c_{1j}c_{m+1,d} = \operatorname{sgn} c_{m+1,1}c_{jd} \neq 0$ by (3.8), it follows that

$$\operatorname{sgn} c_{j,m+1}c_{1d} = -\operatorname{sgn} c_{1j}c_{m+1,d} \neq 0, \text{ or } \operatorname{sgn} c_{1j}c_{m+1,j} = \operatorname{sgn} c_{1d}c_{m+1,d} \neq 0$$

for $1 < j \leqq m$; i.e., whenever $c_{1j}c_{m+1,j} \neq 0$ by Lemma 2.3. Hence, by Lemma 2.1 $V_{m+1,m+1}$ is s.c. with $V_{1,m+1}$; and the lemma is proved.

THEOREM 2. *If a P.a. $C = (c_{ij})$ contains a set of three rows no two of which are proportional, then any given row C_a containing a non-zero element is s.c. with precisely two rows C_f and C_g not proportional to C_a or to each other. C_f and C_g are not s.c. with each other provided that C contains a row not proportional to any of the rows, C_a, C_f, C_g.*

Proof. We may suppose without loss of generality that C_a is C_1, since a P.a. remains a P.a. when the rows are renumbered in any order provided that the columns are also renumbered in that same order, and since sign-compatibility and proportionality of rows is independent of their numbering. First we establish the existence of the rows C_f and C_g when C is irreducible. In the notation of Lemma 2.6 V_{23} and V_{33} are s.c. with V_{13}, since $c_{il} = 0$. When the order of C is $s = 3$, this means that C_2 and C_3 are s.c. with C_1. When $s \geqq 4$, it implies that at least two of the vectors, V_{24}, V_{34}, V_{44}, are s.c. with V_{14} by Lemma 2.6 with $m = 3$. Similarly, applying Lemma 2.6 with $m = 4, 5, \cdots, s-1$ successively, we find distinct integers f and g, $1 < f \leqq s$, $1 < g \leqq s$, such that V_{fs} and V_{gs} are s.c. with V_{1s}; i.e., C_f and C_g are s.c. with C_1. Now suppose C is reducible, containing n rows proportional to C_1 (besides C_1 itself). The minor array obtained by deleting these n rows and the corresponding columns is by Lemma 2.4 a reduction $C^{(n)}$ of C, in which

$C^{(n)}{}_1$ is proportional to no other row. By Lemma 2.5 $C^{(n)}$ has an irreducible reduction $C^{(r)}$, $r \geqq n$, containing at least three rows, one of which is $C^{(r)}{}_1$. As already shown for irreducible arrays, $C^{(r)}$ contains two rows, $C^{(r)}{}_f$ and $C^{(r)}{}_g$, s. c. with $C^{(r)}{}_1$. Hence, by Lemma 2.4, C_f and C_g are s. c. with C_1, and no two of the three are proportional. Next, if there is a row C_h not proportional to any of the rows, C_a, C_f, C_g, then by Lemmas 2.3, 2.1 $\operatorname{sgn} c_{1g}c_{fg} = \operatorname{sgn} c_{1h}c_{fh}$, $\operatorname{sgn} c_{1f}c_{gf} = \operatorname{sgn} c_{1h}c_{gh}$, and hence, $\operatorname{sgn} c_{1g}c_{fh} = \operatorname{sgn} c_{1h}c_{fg} = -\operatorname{sgn} c_{1f}c_{gh}$. Therefore, $\operatorname{sgn} c_{1f}c_{hf}c_{1g}c_{hg} = \operatorname{sgn} c_{f1}c_{g1}c_{fh}c_{gh} = -1$. Thus, C_h cannot be s. c. with C_1, and neither can C_f be s. c. with C_g.

4. The minimax solutions of the general system. If the system (1.2) is consistent and has rank $r > 0$, we can number the equations so that the subsystem,

$$\sum_{j=1}^{n} a_{ij}x_j = a_{i0} \qquad (i = 1, \cdots, r), \tag{4.1}$$

also has rank r. It is then clear that, with respect to any given subset of the unknowns, every minimax solution of (1.2) is a minimax solution of (4.1) and conversely. We, therefore, confine our attention to the system (4.1) with rank equal to the number of equations. Denote the matrix of (4.1) by A; i. e., $A = (a_{ij})$ is an $r \times n$ matrix of rank r. Denote the augmented matrix by $\bar{A}$, the $r \times s$ matrix composed of the columns of $\bar{A}$ with indices $j_1, \cdots, j_s$ in that order by $A_{j_1 \cdots j_s}$, and the determinant of the square matrix $A_{j_1 \cdots j_r}$ by $\alpha_{j_1 \cdots j_r}$. It is sometimes convenient to let J denote the ordered set $(j_1, \cdots, j_q)$, $1 \leqq q \leqq s \leqq n$, and write $A_{Jj_{q+1} \cdots j_s}$ for $A_{j_1 \cdots j_s}$ and similarly for the α's when $s = r$. If J is the null set, we understand $A_{Jj_1 \cdots j_s}$ to be the same as $A_{j_1 \cdots j_s}$. The determinants $\alpha_{j_1 \cdots j_r}$ play an important role in the minimax problem because they are essentially Plücker coordinates for the $(n-r)$-dimensional subspace of intersection of the r hyperplanes (4.1) in projective n-space over F, and they consequently characterize the totality of solutions independently of the particular system of equations through which it is defined. However, we shall derive the required properties of the α's directly without recourse to this geometrical interpretation. Evidently an interchange of subscripts merely changes the sign of $\alpha_{j_1 \cdots j_r}$; and, if two or more subscripts are alike, $\alpha_{j_1 \cdots j_r} = 0$. If $r > 1$ and $J = (j_1, \cdots, j_{r-1})$, we denote the $(r-1)$-rowed square submatrix obtained by deleting the row of index i from A_J by $A^i{}_J$ and its determinant by $\alpha^i{}_J$. We then have

$$\sum_{i=1}^{r} (-1)^{r+i}\alpha^i{}_J a_{ij} = \alpha_{Jj} \qquad (j = 0, \cdots, n). \tag{4.4}$$

LEMMA 3.1. *If* $(X_1, \cdots, X_n)$ *is a solution of the system* (4.1) *and* $J = (j_1, \cdots, j_{r-1})$,

$$\sum_{j=1}^{n} \alpha_{Jj} X_j = \alpha_{J0}. \tag{4.5}$$

Proof. By (4.4)

$$\sum_{j=1}^{n} \alpha_{Jj} X_j = \sum_{j=1}^{n} \sum_{i=1}^{r} (-1)^{r+i} \alpha^i{}_J a_{ij} X_j = \sum_{i=1}^{r} (-1)^{r+i} \alpha^i{}_J \sum_{j=1}^{n} a_{ij} X_j$$

$$= \sum_{i=1}^{r} (-1)^{r+i} \alpha^i{}_J a_{i0} = \alpha_{J0}.$$

By (4.4) if $J = (j_1, \cdots, j_{r-1})$, the last row of the matrix

$$\begin{pmatrix} a_{1k_1} \cdots a_{1k_{r+1}} \\ \cdots\cdots\cdots \\ a_{rk_1} \cdots a_{rk_{r+1}} \\ \alpha_{Jk_1} \cdots \alpha_{Jk_{r+1}} \end{pmatrix}$$

is a linear combination of the first r rows, and hence, the determinant vanishes. Expanding by elements of the last row, we obtain the bilinear relations.

$$\sum_{\nu=1}^{r+1} (-1)^{r+1+\nu} \alpha_{k_1 \cdots k_{\nu-1} k_{\nu+1} \cdots k_{r+1}} \alpha_{j_1 \cdots j_{r-1} k_\nu} = 0. \tag{4.6}$$

LEMMA 3.2. *Let* $K = (k_1, \cdots, k_{r-2})$ *be a sequence of* $r-2$ *distinct integers,* $1 \leqq k_\nu \leqq n$. *Then the array* (α_{Kij}) *for* $i, j = 1, \cdots, n$ *is a Plücker array.*

Proof. Evidently, $\alpha_{Kij} = -\alpha_{Kji}$. Moreover, setting $j_h = k_h$ for $h = 1, \cdots, r-2$, $j_{r-1} = j$, $k_{r-1} = d$, $k_r = e$, $k_{r+1} = f$ in (4.6), we obtain

$$\alpha_{Kef}\alpha_{Kdj} + \alpha_{Kfd}\alpha_{Kej} + \alpha_{Kde}\alpha_{Kfj} = 0. \tag{4.7}$$

Thus, three arbitrarily chosen rows, $(\alpha_{Ki1}, \cdots, \alpha_{Kin})$ for $i = d, e, f$, are linearly dependent.

The following familiar result is stated here for reference.

LEMMA 3.3. *If a matrix* B *has a non-singular* $r \times r$ *submatrix* C *and all* $(r+1) \times (r+1)$ *snbmatrices of* B *that contain* C *are singular, the rank of* B *is* r.

Let $J = (j_1, \cdots, j_{r-1})$ be a sequence of $r-1$ distinct integers, $1 \leqq j_\nu \leqq n$. The number $w(J)$ of zero determinants in the sequence (α_{Jj}), $j = 1, \cdots, n$, we call *the order of* J *with respect to* A. Evidently, $w(J) \geqq r-1$. If $w(J) < n$, we call J a *proper column index sequence* (p. c. i. s.) *for* A. Since

A is of rank $r > 0$, there is a determinant $\alpha_{j_1 \cdots j_r} \neq 0$. Hence, there is always a p.c.i.s. for A. (When $r = 1$, the (only) p.c.i.s. for A is the null set.)

LEMMA 3.4. *$J = (j_1, \cdots, j_{r-1})$ is a p.c.i.s. for A if and only if A_J has maximum rank $r-1$.*

Proof. Let A_J have rank $r-1$ so that, for some integer g, A^g_J is non-singular. Let A' be a matrix obtained by permuting the columns of A so that A_J occupies the first $r-1$ columns. The only $r \times r$ submatrices of A' that contain A^g_J are the matrices A_{Jj} with $j \notin J$. They cannot all be singular, since by Lemma 3.3 the rank of A' would then be $r-1$ instead of r. Hence, at least one of the determinants α_{Jj} does not vanish; so J is a p.c.i.s. for A' and hence, for A. Conversely, if $w(J) < n$, there is an integer f, $1 \leqq f \leqq n$, such that $\alpha_{Jf} \neq 0$ and hence, by (4.4) not all the minors α^i_J are zero. Therefore, the rank of A_J is $r-1$.

LEMMA 3.5. *Let H be a sequence of $q < r$ integers $h_1, \cdots, h_q$, $1 \leqq h_\nu \leqq n$. If the matrix A_H has maximum rank q, then there is a p.c.i.s. for A containing H.*

Proof. Let A_H have rank q. If $q = r-1$, H is itself a p.c.i.s. by Lemma 3.4. Next, let $q = r-1-s$ with $1 \leqq s < r-1$. A_H contains a non-singular $q \times q$ submatrix Q. If every $(q+1) \times (q+1)$ submatrix of A containing Q is singular, then by Lemma 3.3 $r = q$ contrary to hypothesis. Hence, A has a non-singular $(q+1) \times (q+1)$ submatrix Q_1 containing Q. If $s = 1$, the order of Q_1 is $r-1$; and by Lemma 3.4 the indices of the columns of A occurring in Q_1 constitute a p.c.i.s. containing H. If $s > 1$, we repeat the process obtaining a $(q+2) \times (q+2)$ submatrix Q_2 containing Q_1 and therefore Q. After s such steps we obtain a non-singular $(q+s) \times (q+s) = (r-1) \times (r-1)$ submatrix Q_s containing Q, and the indices of the columns of A occurring in Q_s constitute the desired p.c.i.s. containing H.

LEMMA 3.6. *Let the matrix A be such that the sequence $L = (1, 2, \cdots, r-1)$ is a p.c.i.s. of order w and*

$$\alpha_{Lj} = 0 \quad (j = 1, \cdots, w); \qquad \alpha_{Lj} \neq 0 \quad (j = w+1, \cdots, n). \tag{4.8}$$

and let $J = (j_1, \cdots, j_{r-1})$ be a sequence of integers, $1 \leqq j_\nu \leqq w$. Then,

$$\alpha_{Jk} = \theta_J \alpha_{Lk} \qquad (k = 1, \cdots, n). \tag{4.9}$$

where θ_J is an element of F independent of k; namely,

$$\theta_J = \alpha_{Jn}/\alpha_{Ln}. \tag{4.10}$$

Proof. By Lemma 3.4 there is an integer g such that $A^g{}_L$ is non-singular. All the $r \times r$ submatrices of $A_{1\ldots w}$ containing $A^g{}_L$ are singular by (4.8). Hence, by Lemma 3.3 $\alpha_{Jk} = 0$, $k = 1, \cdots, w$; so that, setting $k_h = h$, $h = 1, \cdots, r-1$, $k_r = n$, $k_{r+1} = k$, (4.6) becomes $-\alpha_{Lk}\alpha_{Jn} + \alpha_{Ln}\alpha_{Jk} = 0$. Since L is a p.c.i.s., $\alpha_{Ln} \neq 0$ by (4.8) and the lemma follows.

LEMMA 3.7. *Let A be as in the preceding lemma with the further property that $\alpha^r{}_L \neq 0$, and let $K = (k_1, \cdots, k_{r-2})$ be a sequence of distinct integers, $1 \leqq k_\nu \leqq w$. Then, for each $j = 1, \cdots, n$*

$$\alpha_{Kjk} = \phi_j \alpha^r{}_{Kk} \qquad (k = 1, \cdots, w), \tag{4.11}$$

where ϕ_j is an element of F independent of k; namely,

$$\phi_j = -\alpha_{Lj}/\alpha^r{}_L. \tag{4.12}$$

Proof. By (4.4) and (4.8) we have

$$\alpha^r{}_L \alpha_{Kjk} = \begin{vmatrix} a_{1k_1} & \cdots & a_{1k_{r-2}} & a_{1j} & a_{1k} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{r-1,k_1} & \cdots & a_{r-1,k_{r-2}} & a_{r-1,j} & a_{r-1,k} \\ \alpha_{Lk_1} & \cdots & \alpha_{Lk_{r-2}} & \alpha_{Lj} & \alpha_{Lk} \end{vmatrix} = -\alpha_{Lj}\alpha^r{}_{Kk} \quad (k = 1, \cdots, w)$$

LEMMA 3.8. *With the hypothesis and notation of Lemma 3.7, if K is a p.c.i.s. for $A^r{}_{1\ldots w}$, there is an integer e, $1 \leqq e \leqq w$, such that $\theta_{Ke} \neq 0$ and $\alpha_{Kej} \neq 0$ for $j = w+1, \cdots, n$.*

Proof. Since the order of K with respect to $A^r{}_{1\ldots w}$ is less than w, there is an integer e, $1 \leqq e \leqq w$, such that $\alpha^r{}_{Ke} \neq 0$. Hence, A_{Ke} has maximal rank $r-1$; so by Lemma 3.4 $(k_1, \cdots, k_{r-2}, e)$ is a p.c.i.s. for A. Thus, there is an integer q, $1 \leqq q \leqq n$, such that $\alpha_{Keq} \neq 0$. By Lemma 3.6 $\alpha_{Keq} = \theta_{Ke}\alpha_{Lq}$. Hence, $\theta_{Ke} \neq 0$, and therefore $\alpha_{Kej} = \theta_{Ke}\alpha_{Lj} \neq 0$ for $j = w+1, \cdots, n$ by (4.8).

LEMMA 3.9. *Under the hypothesis of Lemma 3.8 there are integers f and g, $w < f \leqq n$, $w < g \leqq n$, such that all the non-zero members in the set $\{\alpha_{Kgj}\alpha_{Lj}\}$, $j = w+1, \cdots, n$, have the sign of ϕ_g (defined by (4.12)) and all those in the set $\{\alpha_{Kfj}\alpha_{Lj}\}$ have the sign of $-\phi_f$.*

Proof. If $\alpha_{Kij} = 0$ for $i, j = w+1, \cdots, n$, the theorem is trivial. Hence we assume there are integers b and c, $w < b \leqq n$, $w < c \leqq n$, such that $\alpha_{Kbc} \neq 0$. By Lemma 3.8 there is an integer e, $1 \leqq e \leqq w$, such that $\alpha_{Kej} \neq 0$ for $j = w+1, \cdots, n$. Then the array (α_{Kij}) $(i, j = 1, \cdots, n)$, which by Lemma 3.2 is a P.a., contains three rows no two of which are proportional; namely, $R_e = (\alpha_{Ke1}, \cdots, \alpha_{Ken})$, $(\alpha_{Kb1}, \cdots, \alpha_{Kbn})$, $(\alpha_{Kc1}, \cdots, \alpha_{Kcn})$ by Lemma

2.3. Accordingly, by Theorem 2 there are two rows $R_f = (\alpha_{Kf1}, \cdots, \alpha_{Kfn})$ and $R_g = (\alpha_{Kg1}, \cdots, \alpha_{Kgn})$ s.c. with R_e and not proportional to R_e or to each other. By Lemma 2.3

$$\alpha_{Kef}\alpha_{Keg}\alpha_{Kfg} \neq 0; \tag{4.13}$$

and, since $\alpha_{Kek} = 0$ for $k = 1, \cdots, w$ by Lemma 3.7 and eq. (4.8), $f > w$ and $g > w$. Then for any integer j, $w < j \leqq n$, such that $\alpha_{Kfj} \neq 0$, $\operatorname{sgn} \alpha_{Kej}\alpha_{Kfj} = \operatorname{sgn} \alpha_{Keg}\alpha_{Kfg}$ by Lemma 2.1. But by Lemma 3.6 $\alpha_{Kej} = \theta_{Ke}\alpha_{Lj}$ and $\alpha_{Keg} = \theta_{Ke}\alpha_{Lg}$; and therefore, since $\theta_{Ke} \neq 0$ by Lemma 3.8,

$$\operatorname{sgn} \alpha_{Kfj}\alpha_{Lj} = \operatorname{sgn} \alpha_{Kfg}\alpha_{Lg}. \tag{4.14}$$

Likewise for any integer j, $w < j \leqq n$, such that $\alpha_{Kgj} \neq 0$,

$$\operatorname{sgn} \alpha_{Kgj}\alpha_{Lj} = \operatorname{sgn} \alpha_{Kgf}\alpha_{Lf}. \tag{4.15}$$

By Lemma 3.6 and eq. (4.12),

$$\operatorname{sgn}(\alpha_{Kef}\alpha_{Keg}/\alpha^r{}_L) = \operatorname{sgn}(\alpha_{Lf}\alpha_{Lg}/\alpha^r{}_L) = -\operatorname{sgn} \phi_f\alpha_{Lg} = -\operatorname{sgn} \phi_g\alpha_{Lf}. \tag{4.16}$$

By (4.13) one of the expressions, $\alpha_{Kef}\alpha_{Keg}\alpha_{Kfg}$ and $\alpha_{Kef}\alpha_{Keg}\alpha_{Kgf}$, is positive and the other negative. Hence, we may assign the subscripts f and g so that

$$\operatorname{sgn}(\alpha_{Kef}\alpha_{Keg}\alpha_{Kfg}/\alpha^r{}_L) = 1.$$

Therefore, by (4.16), $-\operatorname{sgn} \phi_f\alpha_{Lg}\alpha_{Kfg} = 1$, or $\operatorname{sgn} \alpha_{Kfg}\alpha_{Lg} = -\operatorname{sgn} \phi_f$ so that by (4.14),

$$\operatorname{sgn} \alpha_{Kfj}\alpha_{Lj} = -\operatorname{sgn} \phi_f \tag{4.17}$$

for all non-zero members of the set $\{\alpha_{Kfj}\alpha_{Lj}\}$, $j = w+1, \cdots, n$. Again by (4.16) $-\operatorname{sgn} \phi_g\alpha_{Lf}\alpha_{Kfg} = 1$, or $\operatorname{sgn} \alpha_{Kgf}\alpha_{Lf} = \operatorname{sgn} \phi_g$ so that by (4.15),

$$\operatorname{sgn} \alpha_{Kgj}\alpha_{Lj} = \operatorname{sgn} \phi_g \tag{4.18}$$

for all non-zero members of the set $\{\alpha_{Kgj}\alpha_{Lj}\}$. (4.17) and (4.18) establish the lemma.

Let $J = (j_1, \cdots, j_{r-1})$ be a p.c.i.s. of order w with respect to A, and denote by $j_r, j_{r+1}, \cdots, j_n$ the integers $1, \cdots, n$ not in J in an order such that

$$\alpha_{Jj_\nu} = 0 \quad (\nu = 1, \cdots, w); \qquad \alpha_{Jj_\nu} \neq 0 \quad (\nu = w+1, \cdots, n). \tag{4.19}$$

Hence, the system (4.1) (of rank r) has solutions with arbitrary values assigned to $x_{j_r}, x_{j_{r+1}}, \cdots, x_{j_{n-1}}$. In particular, if we define

$$\mu_J = \alpha_{J0}/\sum_{j=1}^{n} |\alpha_{Jj}|, \qquad \gamma_{Jj} = \mu_J \operatorname{sgn} \alpha_{Jj} \qquad (j = 1, \cdots, n) \tag{4.20}$$

($\sum_{j=1}^{n} |\alpha_{Jj}| \neq 0$ since J is a p.c.i.s. for A), there are elements $X_{j_1}, \cdots, X_{j_w}$ and X_{j_n} in F such that $x_j = \gamma_{Jj}$ for $j = j_{w+1}, \cdots, j_{n-1}$; $x_j = X_j$ for $j = j_1, \cdots, j_w, j_n$ is a solution of (4.1). Then by Lemma 3.1 and eqs. (4.20), (4.19),

$$\alpha_{J0} = \sum_{\nu=1}^{w} \alpha_{Jj_\nu} X_{j_\nu} + \sum_{\nu=w+1}^{n-1} \alpha_{Jj_\nu} \gamma_{Jj_\nu} + \alpha_{Jj_n} X_{j_n} = \mu_J \sum_{\nu=1}^{n-1} |\alpha_{Jj_\nu}| + \alpha_{Jj_n} X_{j_n}$$
$$= \alpha_{J0} + |\alpha_{Jj_n}| (X_{j_n} \operatorname{sgn} \alpha_{Jj_n} - \mu_J).$$

Hence, $X_{j_n} = \mu_J / \operatorname{sgn} \alpha_{Jj_n} = \gamma_{Jj_n}$. We conclude that the system,

$$\sum_{\nu=1}^{w} a_{ij_\nu} x_{j_\nu} = a_{i0} - \sum_{\nu=w+1}^{n} a_{ij_\nu} \gamma_{Jj_\nu} \qquad (i = 1, \cdots, r), \tag{4.21}$$

in $x_{j_1}, \cdots, x_{j_w}$ has the solution $(X_{j_1}, \cdots, X_{j_w})$. The matrix $A_{j_1 \cdots j_w}$ of this system contains a non-singular $(r-1)$-rowed submatrix $A^g{}_J$ by Lemma 3.4; and by (4.19) all the $r \times r$ submatrices of $A_{j_1 \cdots j_w}$ containing $A^g{}_J$ are singular. Hence, by Lemma 3.3 the rank of $A_{j_1 \cdots j_w}$ is $r-1$. The set of equations (4.21) is called the *derived system of* (4.1) *with respect to* J. We have just proved

LEMMA 3.10. *The derived system of* (4.1) *with respect to a p.c.i.s. for* A *is consistent and has rank* $r-1$.

We now define

$$a'_{i0} = a_{i0} - \sum_{j=w+1}^{n} a_{ij} \gamma_{Lj}; \quad \alpha'_{K0} = \begin{vmatrix} a_{1k_1} & \cdots & a_{1k_{r-2}} & a'_{10} \\ \cdots & \cdots & \cdots & \cdots \\ a_{r-1,k_1} & \cdots & a_{r-1,k_{r-2}} & a'_{r-1,0} \end{vmatrix}; \tag{4.22}$$
$$\mu'_K = \alpha'_{K0} / \sum_{k=1}^{w} |\alpha^r{}_{Kk}|$$

where K and L have the meanings assigned in Lemmas 3.6 and 3.8.

LEMMA 3.11. *Under the hypothesis of Lemma* 3.8, *there is an integer* h, $w < h \leqq n$, *such that either* $|\mu_{Kh}| = |\mu'_K|$ or $|\mu_L| \gtrless |\mu_{Kh}| \gtrless |\mu'_K|$.

Proof. By Lemma 3.10 the derived system of (4.1) with respect to the p.c.i.s. $L = (1, \cdots, r-1)$ has a solution $(X_1, \cdots, X_w)$, so that with the notation (4.22)

$$\sum_{k=1}^{w} a_{ik} X_k = a'_{i0} \qquad (i = 1, \cdots, r); \tag{4.23}$$

and, assuming a suitable numbering of equations (4.1), the first $r-1$ equa-

tions of the derived system form a system of rank $r-1$. Applying Lemma 3.1 to this latter system,

$$\sum_{k=1}^{w} \alpha^{r}{}_{Kk} X_k = \alpha'_{K0}. \tag{4.24}$$

Then by Lemma 3.7, eq. (4.24), (4.22), and Lemma 3.7 respectively,

$$\begin{aligned} \sum_{k=1}^{w} \alpha_{Kjk} X_k = \phi_j \sum_{k=1}^{w} \alpha^{r}{}_{Kk} X_k = \phi_j \alpha'_{K0} = \phi_j \mu'_K \sum_{k=1}^{w} |\, \alpha^{r}{}_{Kk} \,| \\ = \mu'_K (\operatorname{sgn} \phi_j) \sum_{k=1}^{w} |\, \alpha_{Kjk} \,| \qquad (j = w+1, \cdots, n). \end{aligned} \tag{4.25}$$

But by (4.23), (4.22), $(X_1, \cdots, X_w, \gamma_{L,w+1}, \cdots, \gamma_{Ln})$ is a solution of (4.1), and by Lemma 3.8 $Kj = (k_1, \cdots, k_{r-2}, j)$ is a p.c.i.s. for A when $w < j \leqq n$. Accordingly,

$$\begin{aligned} \mu_{Kj} \sum_{k=1}^{n} |\, \alpha_{Kjk} \,| = \alpha_{Kj0} = \sum_{k=1}^{w} \alpha_{Kjk} X_k + \sum_{k=w+1}^{n} \alpha_{Kjk} \gamma_{Lk} \\ = \mu'_K (\operatorname{sgn} \phi_j) \sum_{k=1}^{w} |\, \alpha_{Kjk} \,| + \sum_{k=w+1}^{n} \alpha_{Kjk} \gamma_{Lk} \end{aligned} \tag{4.26}$$

for $j = w+1, \cdots, n$ by (4.20), Lemma 3.1, (4.25) respectively. Let f and g be the integers whose existence was established in Lemma 3.9; define $h = f$ if $\mu_L \mu'_K < 0$ and $h = g$ otherwise, so that all non-zero terms in the last member of (4.26) have the same sign for $j = h$. Then we obtain from (4.26)

$$|\, \mu_{Kh} \,| \sum_{k=1}^{n} |\, \alpha_{Khk} \,| = |\, \mu'_K \,| \sum_{k=1}^{w} |\, \alpha_{Khk} \,| + |\, \mu_L \,| \sum_{k=w+1}^{n} |\, \alpha_{Khk} \,|;$$

and hence

$$(|\, \mu_{Kh} \,| - |\, \mu'_K \,|) \sum_{k=1}^{w} |\, \alpha_{Khk} \,| = (|\, \mu_L \,| - |\, \mu_{Kh} \,|) \sum_{k=w+1}^{n} |\, \alpha_{Khk} \,|,$$

from which the lemma follows at once since $\sum_{k=1}^{w} |\, \alpha_{Khk} \,| \neq 0$ by Lemma 3.8.

We now define the *residual submatrix of a system of linear equations* (1.2) *with respect to* $x_{g_1}, \cdots, x_{g_s}$ as the matrix obtained by deleting the columns of index $g_1, \cdots, g_s$ from the matrix of the system, and proceed to state the principal theorem.

THEOREM 3. *Denote the set* $\{1, \cdots, n\}$ *by* N; *let* $G = \{g_1, \cdots, g_s\}$ *be a set of* s *integers of* N, *and write* $H = N - G$. *Let the matrix* A *of the system* (4.1) *have rank* r *equal to the number of equations. Also, if* $s < n$, *let* A_H, *the residual submatrix of* (4.1) *with respect to* $x_{g_1}, \cdots, x_{g_s}$, *have maximum rank. Then the system has the minimax* M^G *with respect to these*

unknowns given by the following: (a) *For* $1 \leqq s \leqq n-r$, $M^G = 0$ *and the minimax solutions with respect to* $x_{g_1}, \cdots, x_{g_s}$ *are the vectors* X^G *such that*

$$X^G{}_j = 0 \quad (j \varepsilon G); \qquad \sum_{j \varepsilon H} a_{ij} X^G{}_j = a_{i0} \qquad (i = 1, \cdots, r). \tag{4.27}$$

(b) *For* $n-r < s \leqq n$, $M^G = \max_J |\mu_J|$, *where* μ_J *is defined by* (4.20) *and* J *ranges over the set* Γ_H *consisting*[4] *of all the p.c.i.s. for* A *that contain* H. *Moreover, let* E *be a p.c.i.s. in* Γ_H *such that* $|\mu_E| = \max_{J \varepsilon \Gamma_H} |\mu_J|$ *and let* D *be the set of integers* $j \varepsilon N$ *such that*

$$\alpha_{Ej} = 0 \quad (j \varepsilon D); \qquad \alpha_{Ej} \neq 0 \qquad (j \varepsilon N - D). \tag{4.28}$$

Then the minimax solutions with respect to $x_{g_1}, \cdots, x_{g_s}$ *are the vectors* X^G *such that*

$$X^G{}_j = \gamma_{Ej} \qquad (j \varepsilon N - D) \tag{4.29}$$

where γ_{Ej} *is defined in* (4.20) *and the remaining components satisfy the equations,*

$$\sum_{j \varepsilon D} a_{ij} X^G{}_j = a_{i0} - \sum_{j \varepsilon N-D} a_{ij} \gamma_{Ej} \qquad (i = 1, \cdots, r), \tag{4.30}$$

and the inequalities,

$$|X^G{}_j| \leqq |\mu_E| \qquad (j \varepsilon D - H). \tag{4.31}$$

Proof. First let $1 \leqq s \leqq n-r$. Then, since the matrix A_H of the coefficients of the unknowns x_j with $j \varepsilon H$ has the same rank r as A and $\bar{A}$, (4.1) has solutions with arbitrary values assigned to the remaining unknowns $x_{g_1}, \cdots, x_{g_s}$. In particular, there is a solution X^G satisfying the conditions (4.27), and the theorem follows at once for this case from the minimax criterion (1.1). For $n-r < s \leqq n$ the proof is by induction on r. For For $r = 1$ (in which case $s = n$) the present theorem reduces to Theorem 1. Next let $r = R > 1$, $n - R < s \leqq n$, and assume that the theorem holds for $r = R-1$, $n-(R-1) < s \leqq n$. For any solution X of (4.1)

$$\sum_{j \varepsilon N-E} \alpha_{Ej} X_j = \alpha_{E0}$$

by Lemma 3.1, since $\alpha_{Ej} = 0$ for $j \varepsilon E$. Applying Lemma 1.1 to this equation and noting that $G = N - H \supseteq N - E$, we find that

$$\max_{j \varepsilon G} |X_j| \geqq \max_{j \varepsilon N-E} |X_j| \geqq |\mu_E|.$$

[4] Γ_H is non-empty by Lemma 3.5. If $s = n$, H is empty and Γ_H is understood to consist of all p.c.i.s. for A.

Then by the minimax criterion (1.1), if there is a solution X^G of (4.1) such that

$$\max_{j \in G} |X^G{}_j| = |\mu_E|, \tag{4.32}$$

then $M^G = |\mu_E|$, and X^G is a minimax solution of (4.1) with respect to $x_{g_1}, \cdots, x_{g_s}$. Moreover, X^G satisfies the conditions (4.29)-(4.31). To verify this last statement note that by Lemma 3.1, (4.28), $x_j = X^G{}_j$ is a solution of the equation, $\sum_{j \in N-D} \alpha_{Ej} x_j = \alpha_{E0}$; and at the same time $\max_{j \in N-D} |X^G{}_j| \leqq |\mu_E|$ by (4.32), since $G \supseteq N - D$. Therefore by Theorem 1 and (4.28), it is a minimax solution of this equation and has components $X^G{}_j$ for $j \in N - D$ given by (4.29). Then, since X^G satisfies (4.1), the remaining components satisfy (4.30); while (4.31) follows from (4.32). Conversely, since $|\gamma_{Ej}| = |\mu_E|$, any vector X^G satisfying (4.29)-(4.31) is a solution of (4.1) for which (4.32) holds. It remains to establish the existence of a vector X^G such that the components $X^G{}_j$ for $j \in D$ satisfy (4.30) and (4.31). For this purpose it is convenient to assume the unknowns numbered so that the subscripts in H are $1, 2, \cdots, n - s$ (unless $s = n$, in which case H is empty); the subscripts in $E - H$ are $n - s + 1, n - s + 2, \cdots, R - 1$ (unless $s = n - R + 1$, in which case $E - H$ is empty); and the subscripts in $D - E$ (if any) are $R, R + 1, \cdots, w$, where w is the order of E with respect to A. Then $E = L = (1, \cdots, R - 1)$, and the equations (4.21) for the derived system of (4.1) with respect to E become

$$\sum_{j=1}^{w} a_{ij} x_j = a_{i0} - \sum_{j=w+1}^{n} a_{ij} \gamma_{Lj} \qquad (i = 1, \cdots, R). \tag{4.33}$$

By Lemma 3.10, assuming a suitable numbering of the equations (4.1), the first $R - 1$ equations (4.33) form a system S' of rank $R - 1$. For $s < n$, if A_H has maximum rank, then the residual matrix $A^R{}_H$ of S' with respect to $x_{n-s+1}, x_{n-s+2}, \cdots, x_w$ also has maximum rank, since the R-th row of A_H is linearly dependent on the other rows. Hence, if $s > n - (R - 1)$, then by the induction hypothesis S' has with respect to these unknowns the minimax, $M' = \max_K |\mu'_K|$ as $K = (k_1, \cdots, k_{R-2})$ ranges over all p.c.i.s. for $A^R{}_{1 \cdots w}$ containing $(1, \cdots, n - s)$. With the specified numbering of the unknowns (4.28) reduces to (4.8), and all the hypotheses of Lemmas 3.6-3.8 and hence, also 3.11 apply to A and each set K with $r = R$. If for any such K, $|\mu'_K| > |\mu_L|$, then by Lemma 3.11 there would be an integer h, $w < h \leqq n$, such that $|\mu_{Kh}| > |\mu_L|$. But, inasmuch as (Kh) is a p.c.i.s. for A by Lemma 3.8 and contains H since K does, we have $|\mu_{Kh}| \leqq \max_{J \in \Gamma_H} |\mu_J| = |\mu_E|$

$= |\mu_L|$. Hence, $M' = \max_K |\mu'_K| \leqq |\mu_L|$ for $s > n-(R-1)$. This holds for $s = n-(R-1)$ also, since in that case S' has the minimax $M' = 0$ with respect to $x_{n-s+1}, \cdots, x_w$, as we find by applying the present theorem for $s \leqq n-r$, in which case it has already been proved. Now, if $(X^G{}_1, \cdots, X^G{}_w)$ is any solution of S', then by Lemma 3.10 it satisfies all the equations (4.33) and hence, also with the specified numbering the conditions (4.30). If in addition it is a minimax solution of S' with respect to $x_{n-s+1}, \cdots, x_w$, then $|X^G{}_j| \leqq M' \leqq |\mu_L|$ for $j = n-s+1, \cdots, w$, and with the specified numbering this is equivalent to (4.31). That is, we obtain the required vector X^G by choosing $(X^G{}_1, \cdots, X^G{}_w)$ as a minimax solution of S' with respect to $x_{n-s+1}, \cdots, x_w$. Thus, the theorem is proved for $r = R$, $n-R < s \leqq n$, and the induction is complete.

We remark that in determining $\max_J |\mu_J|$ it is sufficient to consider sequences $J = (j_1, \cdots, j_{r-1})$ with $j_1 < j_2 < \cdots < j_{r-1}$, since the value of $|\mu_J|$ is independent of the order of the indices in J.

COROLLARY 3. *For $n-r < s \leqq n$, if $D = E = (e_1, \cdots, e_{r-1})$; i.e., if the determinants α_{Ej} vanish only for $j \varepsilon E$, there is a single minimax solution X^G, the components $X^G{}_j$ for $j \varepsilon E$ being uniquely determined by the equations* (4.30) *alone. In the notation of* (4.22) *with E in place of L and the equations* (4.1) *numbered so that the forms $\sum_{j \varepsilon E} a_{ij}x_j$ $(i = 1, \cdots, r-1)$ are linearly independent, this solution is explicitly given by the equations,*

$$X^G{}_{e_k} = \alpha'_{e_1 \cdots e_{k-1} 0 e_{k+1} \cdots e_{r-1}} / \alpha^r{}_E \quad (k = 1, \cdots, r-1); \qquad X^G{}_j = \gamma_{Ej} \quad (j \varepsilon N - E).$$

There remains the case that the residual matrix in question does not have maximum rank. This can be treated by means of the following theorem.

THEOREM 4. *Let the matrix A of the system* (4.1) *have rank r equal to the number of equations. In the notation of Theorem* 3, *if $s < n$ and A_H, the residual matrix with respect to $x_{g_1}, \cdots, x_{g_s}$, has rank $t < \min(r, n-s)$, let T be a sequence of t integers out of H such that A_T has maximum rank t. Then* (4.1) *has the same minimax with respect to $x_{g_1}, \cdots, x_{g_s}$ as the system,*

$$\sum_{j \varepsilon T+G} a_{ij}u_j = a_{i0} \qquad (i = 1, \cdots, r), \tag{4.34}$$

has with respect to $u_{g_1}, \cdots, u_{g_s}$ (and the latter minimax can be determined by Theorem 3). *For each $k \varepsilon H - T$ there are elements c_{kj} such that*

$$\sum_{j \varepsilon T} a_{ij}c_{kj} = a_{ik} \qquad (i = 1, \cdots, r). \tag{4.35}$$

Each minimax solution X^G of (4.1) *can be derived from a corresponding minimax solution U^G of* (4.34) *by assigning arbitrary values to the components $X^G{}_j$ with $j \in H - T$ and determining the remaining components by means of the equations,*

$$(4.36) \qquad X^G{}_j = U^G{}_j \quad (j \in G), \qquad X^G{}_j = U^G{}_j - \sum_{k \in H-T} c_{kj} X^G{}_k \quad (j \in T).$$

Proof. For any integer $k \in H - T$ the augmented matrix of (4.35) (considered as a system of equations in the unknowns c_{kj}), being the same as a submatrix of A_H except possibly for a permutation of columns, has the same rank t as the matrix A_T of the system. Consequently there are elements c_{kj} satisfying (4.35). If X is a solution of (4.1) and elements U_j are given by

$$(4.37) \qquad U_j = X_j \quad (j \in G), \qquad U_j = X_j + \sum_{k \in H-T} c_{kj} X_k \quad (j \in T),$$

then $u_j = U_j$ is a solution of (4.34), since by (4.37), (4.35)

$$\sum_{j \in T} a_{ij} U_j = \sum_{j \in T} a_{ij} X_j + \sum_{j \in T} \sum_{k \in H-T} a_{ij} c_{kj} X_k = \sum_{j \in T} a_{ij} X_j + \sum_{k \in H-T} a_{ik} X_k = \sum_{j \in H} a_{ij} X_j.$$

Conversely, if $u_j = U_j$ is a solution of (4.34) and elements X_j for $j \in H - T$ are chosen arbitrarily, then elements X_j for $j \in T + G$ are uniquely determined by (4.37) and the resulting vector $(X_1, \cdots, X_n)$ is a solution of (4.1). In particular, if $u_j = U^G{}_j$ is a minimax solution of (4.34), then the vector X^G given by (4.36) with $X^G{}_j$ arbitrary for $j \in H - T$ is a solution of (4.1). Moreover, it is a minimax solution; for, if X is any other solution of (4.1) and the elements U_J are determined by (4.37), then, as noted above, $u_j = U_j$ is a solution of (4.34) and hence,

$$\max_j |X_j| = \max_j |U_j| \geqq \max_j |U^G{}_j| = |\max_j |X^G{}_j| \qquad (j \in G).$$

Conversely, X^G is a minimax solution of (4.1) only if the elements $U^G{}_j$ determined by (4.36) are the components of a minimax solution U^G of (4.34). Finally, the matrix of the system (4.34) has rank r equal to the number of equations, since it is obtained from A by deleting columns linearly dependent on those occurring in A_T; and the residual matrix with respect to $u_{g_1}, \cdots, u_{g_s}$ is A_T, which has maximum rank by hypothesis. Accordingly, (4.34) does indeed have a minimax solution U^G by Theorem 3. Hence, (4.1) has a minimax solution X^G and for both systems $M^G = \max_j |X^G{}_j| = \max_j |U^G{}_j|$ $(j \in G)$.

5. The minimax of a system of linear functions. The minimax and minimax points of a system of linear functions over F,

$$(5.1) \qquad L_i(x_1, \cdots, x_q) = \sum_{j=1}^{q} b_{ij}x_j - b_{i0} \qquad (i = 1, \cdots, r),$$

can be determined by applying the theorems of the preceding section to the system of linear equations,

$$(5.2) \qquad \sum_{j=1}^{q} b_{ij}x_j - \sum_{j=q+1}^{q+r} \delta_{q+i,j}x_j = b_{i0} \qquad (i = 1, \cdots, r),$$

where δ_{hj} is the unit element of F when $h = j$ and is the zero element otherwise. All solutions of (5.2) are given by

$$(5.3) \qquad x_j = X_j \quad (j = 1, \cdots, q), \qquad x_j = L_{j-q}(X_1, \cdots, X_q) \quad (j = q+1, \cdots, q+r),$$

in which $X_1, \cdots, X_q$ are arbitrary elements of F. Consequently, the minimax $M^*(L)$ of (5.1) is the same as the minimax of (5.2) with respect to $x_{q+1}, \cdots, x_{q+r}$. Moreover, $(X^*_1, \cdots, X^*_q)$ is a minimax point and $(L^*_1, \cdots, L^*_r)$ a minimax vector of (5.1) if and only if $(X^*_1, \cdots, X^*_q, L^*_1, \cdots, L^*_r)$ is a minimax solution of (5.2) with respect to $x_{q+1}, \cdots, x_{q+r}$.

For convenient expression of the results we introduce some additional notations. If the rows of index $i_1, \cdots, i_s$ are deleted from a matrix B, we denote the resulting matrix by $B^{i_1 \cdots i_s}$. If the superscripts are all distinct and the latter matrix is square, $\beta^{i_1 \cdots i_s}$ is its determinant and otherwise is zero. Let B be $r \times q$ and, if $q < r$, let $I = (i_1, \cdots, i_{r-q-1})$ be a sequence of $r - q - 1$ distinct integers, $1 \leqq i_\nu \leqq r$. The number $d(I)$ of zeros in the sequence $(\beta^{I1}, \cdots, \beta^{Ir})$ we call the *degree of I with respect to B*. Clearly, $d(I) \geqq r - q - 1$. If $d(I) < r$, we call I a *proper row index* sequence (p. r. i. s.) *for B*.

THEOREM 5. *Let the matrix $B = (b_{ij})$ $(i = 1, \cdots, r; j = 1, \cdots, q)$ of the system of linear functions* (5.1) *have maximum rank, and denote by B_0 the matrix obtained from B by adjoining the elements b_{i0} as the $(q+1)$-th column. Then the system* (5.1) *has a minimax $M^*(L)$. If $q \geqq r$, $M^*(L) = 0$ and the minimax points X^* are those for which $L_i(X^*_1, \cdots, X^*_q) = 0$ $(i = 1, \cdots, r)$. If $q < r$, $M^*(L) = \max_I |\mu^I|$, where I ranges over all p. r. i. s. for B and μ^I is defined by*

$$\mu^I = \beta_0{}^I / \sum_{i=1}^{r} |\beta^{Ii}|.$$

Let V be a p. r. i. s. such that $|\mu^V| = \max_I |\mu^I|$; let R denote the set $\{1, \cdots, r\}$, U the set of integers $i \in R$ such that $\beta^{Vi} = 0$, and $\varepsilon(V, i)$ the number of

integers in V exceeding i. Then the minimax points X^* are those which satisfy the conditions,

$$(5.4) \qquad L_i(X^*_1, \cdots, X^*_q) = (-1)^{r-1+i+\varepsilon(V,i)}\mu^V \operatorname{sgn}\beta^{Vi} \qquad (i \varepsilon R - U).$$

$$(5.5) \qquad |L_i(X^*_1, \cdots, X^*_q)| \leqq |\mu^V| \qquad (i \varepsilon U).$$

Proof. For $q \geqq r$ the theorem is immediate. To establish it in the case $q < r$ we proceed to determine the minimax M^G of (5.2) with respect to $x_{q+1}, \cdots, x_{q+r}$, using the notation of Section 4 with $a_{ij} = b_{ij}$ for $j = 0, 1, \cdots, q$ and $a_{ij} = -\delta_{q+i,j}$ for $j = q+1, \cdots, q+r$. The rank of the matrix A of (5.2) turns out to be r, the same as the number of equations; and the residual matrix with respect to these unknowns is B, which has maximum rank by hypothesis. Thus, M^G can be determined by the case $n - r < s \leqq n$ of Theorem 3. Noting that for a sequence of integers $I = (i_1, \cdots, i_{r-q-1})$ with $1 \leqq i_1 < i_2 < \cdots < i_{r-q-1} \leqq r$

$$\alpha_{1\ldots q, q+i_1, \ldots, q+i_{r-q}} = (-1)^p \beta^{I i_{r-q}},$$

$$p = \tfrac{1}{2}(r-q)(r+q+3) + i_1 + \cdots + i_{r-q} + \varepsilon(I, i_{r-q})$$

$$\alpha_{1\ldots q, q+i_1, \ldots, q+i_{r-q-1}, 0} = (-1)^{p_0}\beta_0{}^I,$$

$$p_0 = \tfrac{1}{2}(r-q-1)(r+q+2) + i_1 + \cdots + i_{r-q-1}$$

and hence, that J is a p.c.i.s. for A containing $H = \{1, \cdots, q\}$ if and only if $J = \{1, \cdots, q, q+i_1, \cdots, q+i_{r-q-1}\}$ and I is a p.r.i.s. for B, we have $\mu_J = (-1)^{p_0}\mu^I$ for $J \varepsilon \Gamma_H$. Consequently, M^G and hence, also $M^*(L)$ is $\max_I |\mu^I|$ as I ranges over the p.r.i.s. for B. Moreover, letting

$$V = (v_1, \cdots, v_{r-q-1}) \text{ and } E = \{1, \cdots, q, q+v_1, \cdots, q+v_{r-q-1}\},$$

we have $|\mu_E| = \max_{J \varepsilon \Gamma_H} |\mu_J|$. Hence, in the notation of Theorem 3, $q + i \varepsilon D - H$ is equivalent to $i \varepsilon U$, and $q + i \varepsilon N - D$ is equivalent to $i \varepsilon R - U$, since $\alpha_{E,q+i} = 0$ if and only if $\beta^{Vi} = 0$. Then for any minimax vector X^* of (5.1) and any minimax solution X^G of (5.2) it follows from (4.29) that

$$L_i(X^*_1, \cdots, X^*_q) = X^G{}_{q+i} = \gamma_{Eq+i} = \mu_E \operatorname{sgn}\alpha_{Eq+i}$$

$$= (-1)^{r-1+i+\varepsilon(V,i)}\mu^V \operatorname{sgn}\beta^{Vi} \qquad (i \varepsilon R - U),$$

and from (4.31) that

$$|L_i(X^*_1, \cdots, X^*_q)| = |X^G{}_{q+i}| \leqq |\mu_E| = |\mu^V| \qquad (i \varepsilon U).$$

Since (4.30) is then satisfied automatically, the conditions (5.4), (5.5) characterize the minimax points X^* completely.

COROLLARY 5. *If $U = V$, i.e. if none of the determinants β^{Vi} $(i \notin V)$ vanish, the system* (5.1) *has a unique minimax point X^*, namely, the (in this case) unique solution of* (5.4).

To determine the minimax of (5.1) when the matrix B does not have maximum rank, we employ Theorem 4 and obtain

THEOREM 6. *Let the rank of B be $t < \min(q, r)$, and let T be a set of t integers out of $H = \{1, \cdots, q\}$ such that the submatrix B_T has maximum rank t. Then* (5.1) *has the same minimax as the system,*

$$\sum_{j \in T} b_{ij} u_j - b_{i0} \qquad (i = 1, \cdots, r) \tag{5.6}$$

with matrix of miximum rank. For each $k \in H - T$ there are elements c_{kj} such that

$$\sum_{j \in T} b_{ij} c_{kj} = b_{ik} \qquad (i = 1, \cdots, r).$$

Each minimax point X^* of (5.1) *can be derived from a corresponding minimax point U^* of* (5.6) *by assigning arbitrary values to the components X^*_j with $j \in H - T$ and determining the remaining components by means of the equations,*

$$X^*_j = U^*_j - \sum_{k \in H-T} c_{kj} X^*_k \qquad (j \in T).$$

6. Problems in best approximation. The foregoing results can be applied to certain problems of best approximation in the Tchebycheff sense. For example, if as an alternative to the usual least squares criterion we define a *best approximate solution* x^* of an inconsistent system of linear equations,

$$\sum_{j=1}^{q} b_{ij} x_j = b_{i0} \qquad (i = 1, \cdots, r),$$

as a set of values for x which minimizes the largest of the "errors" $|\sum_j b_{ij} x_j - b_{i0}|$ $(i = 1, \cdots, r)$, then the vectors x^* are precisely the minimax points of the system of linear functions (5.1) and hence, are determined by Theorems 5 and 6.

Next we consider the problem of best approximation to a function at a finite number of points. Let S_p be a set of p points $x_1, \cdots, x_p$ in a completely arbitrary space, and let Φ be the class of all single-valued functions defined on S_p with range in the ordered field F. Given a subclass G of Φ and a function $\phi(x) \in \Phi$, we define a *G-function of best approximation to ϕ on S_p* as a function $g^*(x) \in G$ which minimizes $\max_{x \in S_p} |g(x) - \phi(x)|$ as g ranges

over G. If $g_1(x), \cdots, g_q(x)$ are given functions in Φ and we take G as the class of functions expressible in the form $\sum_{j=1}^{q} c_j g_j(x)$ with $c_j \in F$, then[5] $g^*(x) = \sum_{j=1}^{q} c^*_j g_j(x)$, where $(c^*_1, \cdots, c^*_q)$ is a minimax point of the system of linear functions,

$$L_i(c_1, \cdots, c_q) = \sum_{j=1}^{q} c_j g_j(x_i) - \phi(x_i) \qquad (i = 1, \cdots, p),$$

and so again is determined by Theorems 5 and 6. The particular cases $g_j(x) = x^j$ and $g_{2k}(x) = \cos kx$, $g_{2k+1}(x) = \sin kx$ yield the results of De La Vallée Poussin [5] on best approximation on sets of p real numbers by polynomials of degree $n = q - 1 \leqq p - 2$ and by trigonometric sums of order $n = (q-1)/2 \leqq (p-2)/2$ respectively, if we note that in these cases none of the determinants β^{Ii} vanish so that Corollary 5 is applicable and there is a unique minimax point.

Finally, we determine the G-function of best approximation to ϕ on S_p when G is the class of all functions $g \in \Phi$ whose values on S_p are subject to a set of linear conditions,

$$\sum_{j=1}^{p} c_{ij} g(x_j) = c_{i0} \qquad (i = 1, \cdots, r), \tag{6.1}$$

in which the c_{ij} are given elements of F. An important instance is the class of all functions in Φ whose n-th divided differences on S_p have preassigned values, $[x_i, x_{i+1}, \cdots, x_{i+n}] = c_{i0}$ for $i = 1, \cdots, p - n$. Then (6.1) holds with $p = r + n$,

$$c_{ij} = \prod_{k} (x_j - x_k)^{-1} (k = i, i+1, \cdots, j-1, j+1, \cdots, i+n)$$

for $j = i, i+1, \cdots, i+n$ and $c_{ij} = 0$ otherwise,[6] provided S_p is a subset of F. For this choice of the class of approximating functions the values $g^*(x)$ on S_p are given by

$$g^*(x_j) = Y^*_j + \phi(x_j) \qquad (j = 1, \cdots, p),$$

where $y = Y^*$ is any minimax solution of the system of linear equations,

$$\sum_{j=1}^{p} c_{ij} y_j = c_{i0} - \sum_{j=1}^{p} c_{ij} \phi(x_j) \qquad (i = 1, \cdots, r),$$

and can therefore be obtained by means of Theorems 3 and 4.

UNIVERSITY OF GEORGIA.

[5] This problem has recently been treated for $q = p - 1$ in the field of complex numbers by T. S. Motzkin and J. L. Walsh [8].

[6] See for example [7].

REFERENCES.

[1] Hans Rademacher and I. J. Schoenberg, "Helly's theorem on convex domains and Tchebycheff's approximation problem," *Canadian Journal of Mathematics*, vol. 2 (1950), pp. 251-252.

[2] V. K. Ivanov, "The problem of the minimax of a system of linear functions," *Mat. Sbornik N. S.* 28(70) (1951), pp. 685-706 (Russian); English abstract in *Mathematics Review*, vol. 13 (1952), p. 119.

[3] N. Ahiezer and M. Krein, *On Some Problems of the Theory of Moments*, Harkov, 1938 (Russian), pp. 171-199.

[4] E. Ya. Remez, "On Chebyshev approximations in a complex region," *Doklady Akad. Nauk SSSR* (N.S.), vol. 77 (1951), pp. 965-968 (Russian); English abstract in *Mathematics Review*, vol. 13 (1952), p. 99.

[5] C. de la Vallée Poussin, *Leçons sur l'approximation des fonctions d'une variable réelle*, Paris, 1919, Chapters VI and VII.

[6] M. Bôcher, *Introduction to Higher Algebra*, New York, 1907, p. 54.

[7] T. Fort, *Finite Differences*, Oxford, 1948, p. 10.

[8] T. S. Motzkin and J. L. Walsh, "On the derivative of a polynomial and Chebyshev approximation," *Proceedings of the American Mathematical Society*, vol. 4 (1953), pp. 76-87.

CONVERGENCE IN AREA OF INTEGRAL MEANS.*[1]

By CASPER GOFFMAN[2]

The integral means $f_n(x,y) = n^2 \int_0^{1/n} \int_0^{1/n} f(x+u, y+v)\,du\,dv$, $n = 1, 2, \cdots$, of a function $f(x,y)$ have been used as a smoothing approximation to $f(x,y)$ in a variety of applications. Their use in surface area theory seems to have been first made by T. Radó, [1], who showed, for continuous $f(x,y)$, that the Lebesgue areas, $A(f_n)$, of the surfaces given by $f_n(x,y)$, $n = 1, 2, \cdots$, converge to the Lebesgue area $A(f)$ of the surface given by $f(x,y)$.

For summable $f(x,y)$, the Lebesgue area is in general meaningless and, in previous papers, L. Cesari [2] and the author [3] have introduced, in different ways, generalized Lebesgue areas, $\Phi_C(f)$ and $\Phi(f)$, which were proved in [3] to coincide for every summable $f(x,y)$. Our main purpose is to show that the result of Radó mentioned above concerning the $f_n(x,y)$ holds for every summable $f(x,y)$ provided the Lebesgue area is replaced by the generalized Lebesgue area. Indeed, for every summable $f(x,y)$, the integral means $f_n(x,y)$ are continuous so that their Lebesgue areas $A(f_n)$ do exist. What we show is that the sequence $\{A(f_n)\}$ either converges, or diverges to $+\infty$; i.e., it converges on the extended closed interval $[0, +\infty]$, and the limit coincides with the generalized Lebesgue area:

$$\lim_{n\to\infty} A(f_n) = \Phi(f) = \Phi_C(f).$$

It follows that the limit above can itself be interpreted as a definition of "the area of the surface defined by $f(x,y)$."

The area $H(f)$ of the paper [3], where we proved that $\Phi_C = \Phi = H$, is denoted by $\chi(f)$ in the present paper. The area $\Phi(f)$ of the present paper was not considered in [3] and we prove that $\Phi(f) = \chi(f)$.

For convenience, we say that a function $f(x,y)$ has *property R* if the sequence $\{A(f_n)\}$ of Lebesgue areas of its integral means converges on the interval $[0, +\infty]$. We thus show that every summable $f(x,y)$ has property

* Received November 3, 1954.

[1] Research supported by a grant from the National Science Foundation.

[2] We are grateful to the referee for his thoughtful criticism of the first version of this paper.

R. The property R is defined similarly for representations of parametric curves and surfaces. We shall show also that every $f: x_i(t)$, $i=1,2$, $0 \leqq t \leqq 1$, $x_i(t)$ summable, has property R. For parametric surfaces, the situation is difficult, as may be expected. For this case, we extend a result of C. B. Morrey [4], [5], [6], but shall omit the proofs since they are essentially the same as for the continuous case.

We first show that property R is general for curves; i.e., if $x(t)$, $y(t)$ are summable functions on the closed interval $[0,1]$, with integral means $x_n(t) = n\int_0^{1/n} x(t+u)du$ and $y_n(t) = n\int_0^{1/n} y(t+u)du$, $n=1,2,\cdots$, then the sequence of lengths of the curves given by $x_n(t)$, $y_n(t)$ converges on the closed interval $[0,+\infty]$.

The generalized variation $\phi(x)$ of a summable function $x(t)$, on $[0,1]$, was defined in [3]. One of several equivalent definitions is the following:

For any finite set $S: 0 < t_0 < t_1 < \cdots < t_n < 1$, let the norm, $\nu(S)$, be the largest of the numbers $t_0, t_1 - t_0, \cdots, 1 - t_n$. Let

$$\phi(x;S) = \sum_{i=1}^{n} |x(t_i) - x(t_{i-1})|.$$

Now, let E be the set of points of approximate continuity of $x(t)$, and let $\phi(x) = \sup \phi(x;S)$ for all $S \subset E$. The following result is a simple consequence of this definition:

If $\phi(x) < +\infty$, then for every $\epsilon > 0$ there is a $\delta > 0$ such that $S \subset E$ and $\nu(S) < \delta$ implies $\phi(x;S) > \phi(x) - \epsilon$. If $\phi(x) = +\infty$ then for every $M > 0$ there is a $\delta > 0$ such that $S \subset E$ and $\nu(S) < \delta$ implies $\phi(x;S) > M$.

The function $\phi(x)$ agrees with the variation $V(x)$ for continuous $x(t)$ but not necessarily for discontinuous $x(t)$. However, it is always true that $\phi(x) \leqq V(x)$.

The integral means

$$x_n(t) = n\int_0^{1/n} x(t+u)du \text{ and } y_n(t) = n\int_0^{1/n} y(t+u)du$$

are defined on the interval $[0, 1-1/n]$, are absolutely continuous, and so are differentiable almost everywhere. It follows by the fundamental theorem of Lebesgue integration that the derivatives are given almost everywhere by

$$x_n'(t) = n\{x(t+1/n) - x(t)\} \text{ and } y_n'(t) = n\{y(t+1/n) - y(t)\}$$

so that, since $x_n(t)$ and $y_n(t)$ are absolutely continuous,

$$\phi(x_n) = V(x_n) = \int_0^{1-1/n} |x_n'(t)|\,dt = n\int_0^{1-1/n} |x(t+1/n) - x(t)|\,dt$$

and

$$\phi(y_n) = n\int_0^{1-1/n} |\, y(t+1/n) - y(t)\,|\, dt.$$

We show that the sequences $\{\phi(x_n)\}$ and $\{\phi(y_n)\}$ converge on the closed interval $[0, +\infty]$. It is only necessary to show this for $\{\phi(x_n)\}$.

Let us first prove that $\phi(x_n) \leqq \phi(x)$. Indeed, we have

$$\begin{aligned}\phi(x_n) &= n\int_0^{1-1/n} |\, x(t+1/n) - x(t)\,|\, dt \\ &= n\int_0^{1/n} \sum_{i=1}^{n-1} |\, x(t+i/n) - x(t+(i-1)/n)\, dt.\end{aligned}$$

For almost all t, $0 \leqq t \leqq 1/n$, the points $t,\ t+1/n, \cdots, t+(n-1)/n$ are all points of approximate continuity for $x(t)$, and hence, the sum under the last integral does not exceed $\phi(x)$. Thus:

$$\phi(x_n) \leqq n\int_0^{1/n} \phi(x)\, dt = \phi(x).$$

Suppose $\phi(x) < \infty$. Let $\epsilon > 0$. By the above remark, there is a $\delta > 0$ such that $S \subset E$ and $\nu(S) < \delta$ imply $\phi(x; S) > \phi(x) - \epsilon$. But, for all $n > 1/\delta$, and all $t \in [0, 1/n]$, the set $t, t+1/n, \cdots, t+(n-1)/n$ has norm less than δ and, for almost all t, it is a subset of E, so that

$$\phi(x) - \epsilon < \sum_{i=1}^{n-1} |\, x(t+i/n) - x(t+(i-1)/n)\,|.$$

Hence,

$$\begin{aligned}\phi(x) - \epsilon &< n\int_0^{1/n} \sum_{i=1}^{n-1} |\, x(t+i/n) - x(t+(i-1)/n)\,|\, dt \\ &= n\int_0^{1-1/n} |\, x(t+1/n) - x(t)\,|\, dt = \phi(x_n).\end{aligned}$$

Thus, for every $n > 1/\delta$, we have $\phi(x) - \epsilon < \phi(x_n) \leqq \phi(x)$, so that $\{\phi(x_n)\}$ converges to $\phi(x)$. If $\phi(x) = +\infty$, a similar argument shows that $\{\phi(x_n)\}$ converges to $+\infty$.

Now, for each n, the pair $x_n(t)$, $y_n(t)$ represents a continuous curve C_n whose length is given by

$$\begin{aligned}L(C_n) &= \int_0^{1-1/n} [x_n'(t)^2 + y_n'(t)^2]^{\frac{1}{2}}\, dt \\ &= n\int_0^{1-1/n} [\{x(t+1/n) - x(t)\}^2 + \{y(t+1/n) - y(t)\}^2]^{\frac{1}{2}}\, dt \\ &= n\int_0^{1/n} \sum_{i=1}^{n-1} [\{x(t+i/n) - x(t+(i-1)/n)\}^2 \\ &\qquad + \{y(t+i/n) - y(t+(i-1)/n)\}^2]^{\frac{1}{2}}\, dt.\end{aligned}$$

If, now, E is the set of points at which both $x(t)$ and $y(t)$ are approximately continuous, and f is the pair $x(t)$, $y(t)$, we may let

$$\psi(f;S)=\sum_{i=1}^{n}[\{x(t_i)-x(t_{i-1})\}^2+\{y(t_i)-y(t_{i-1})\}^2]^{\frac{1}{2}}$$

for each $S: 0<t_0<t_1<\cdots<t_n<1$ and then let $\psi(f)=\sup\psi(f;S)$ for all $S\subset E$. As for $\phi(f)$, we again have: If $\psi(f)<+\infty$, then for every $\epsilon>0$ there is a $\delta>0$ such that if $\nu(S)<\delta$, and $S\subset E$, then $\psi(f;S)>\psi(f)-\epsilon$; if $\psi(f)=+\infty$, then for every $M>0$ there is a $\delta>0$ such that if $\nu(S)>\delta$, and $S\subset E$, then $\psi(f;S)>M$.

It then follows, just as for $\phi(x)$, that if $\psi(f)<+\infty$ then for every $\epsilon>0$ there is an N such that $n>N$ implies $\psi(f)-\epsilon<L(C_n)<\psi(f)$, and if $\psi(f)=+\infty$, for every $M>0$ there is an N such that $n>N$ implies $L(C_n)>M$. We may now state:

THEOREM 1. *If $x(t)$, $y(t)$ are summable functions defined on $[0,1]$, and C_n is the curve corresponding to the integral means $x_n(t)=n\int_0^{1/n}x(t+u)\,du$, $y_n(t)=n\int_0^{1/n}y(t+u)\,du$, $n=1,2,\cdots$, then the sequence $\{L(C_n)\}$ of lengths converges on $[0,+\infty]$. In other words, every summable $x(t)$, $y(t)$ has property R.*

Let $f(x,y)$ be a summable function defined on the unit square $I=[0,1]\times[0,1]$. For every natural number n, the integral mean $f_n(x,y)=n^2\int_0^{1/n}\int_0^{1/n}f(x+u,y+v)\,du\,dv$ is defined on the square

$$I_n=[0,1-1/n]\times[0,1-1/n].$$

It is continuous, and is absolutely continuous in each variable for almost all values of the other variable; moreover, it is well known, and easy to prove, that its partial derivatives are given almost everywhere by the expressions

$$(1)\qquad \partial f_n(x,y)/\partial x=n^2\int_0^{1/n}\{f(x+1/n,y+v)-f(x,y+v)\}\,dv$$

$$(2)\qquad \partial f_n(x,y)/\partial y=n^2\int_0^{1/n}\{f(x+u,y+1/n)-f(x+u,y)\}\,du.$$

For continuous $f(x,y)$, [5], the derivatives $\partial f_n/\partial x$, $\partial f_n/\partial y$ are given everywhere by (1) and (2) and it is obvious that they are continuous.

It follows easily that $\partial f_n/\partial x$ and $\partial f_n/\partial y$ are summable. For:

$$\int_0^{1-1/n}\int_0^{1-1/n} |\partial f_n/\partial x|\, dx\, dy$$

$$= \int_0^{1-1/n}\int_0^{1-1/n} \{n^2 \int_0^{1/n} |f(x+1/n, y+v) - f(x, y+v)|\, dv\}\, dx\, dy$$

$$\leqq n^2 \int_0^{1/n} dv \{\int_0^{1-1/n}\int_0^{1-1/n} [|f(x+1/n, y+v)| + |f(x, y+v)]dx\, dy\}$$

$$\leqq 2n^2 \int_0^{1/n} dv \int_0^1 \int_0^1 |f(x, y)|\, dx\, dy = 2n \int_0^1 \int_0^1 |f(x, y)|\, dx\, dy,$$

and the result follows since $f(x, y)$ is summable.

Moreover, since $f_n(x, y)$ is absoluately continuous in each variable for all values of the other variable, it is ACT and so:

If $f(x, y)$ is summable, the surfaces given by the integral means $f_n(x, y)$, $n = 1, 2, \cdots$, all have finite Lebesgue areas given by

$$(3) \quad A(f_n) = \int_0^{1-1/n}\int_0^{1-1/n} [1 + \{n^2 \int_0^{1/n} (f(x+1/n, y+v) - f(x, y+v))dv\}^2$$

$$+ \{n^2 \int_0^{1/n} (f(x+u, y+1/n) - f(x+u, y))du\}^2]^{\frac{1}{2}}\, dx\, dy.$$

We shall show that the sequence (3) converges on the closed interval $[0, +\infty]$. It seems worth noting that the technique used in proving Theorem 1 now yields an inequality instead of an equality. Thus, a separate argument is needed to prove the opposite inequality. Since $f(x, y)$ is measurable, there are subsets E_x and E_y of $[0, 1]$, each of measure 1, such that for every $x \in E_x$, $y \in E_y$, $f(x, y)$ is approximately continuous almost everywhere in the other variable.

Just as we did in the case of functions of one variable, we first prove our result for variation functions $\Phi_1(f)$ and $\Phi_2(f)$, which we now define. Let $\phi(f; x; c, d)$ be the generalized variation of $f(x, y)$ for x fixed and y varying on the interval $[c, d]$, and let $\phi(f; y; a, b)$ have similar meaning. We note that these functions are essentially additive; i.e., if $c < c' < d$ and $f(x, y)$ is approximately continuous in y at the point (x, c'), then

$$\phi(f; x; c, c') + \phi(f; x; c', d) = \phi(f; x; c, d).$$

We let

$$\Phi_1(f; a, b; c, d) = \int_a^b \phi(f; x; c, d)dx \quad \text{and} \quad \Phi_2(f; a, b; c, d) = \int_c^d \phi(f; y; a, b)dy.$$

In particular, we write,

$$\Phi_1(f) = \Phi_1(f; 0, 1; 0, 1) \quad \text{and} \quad \Phi_2(f) = \Phi_2(f; 0, 1; 0, 1).$$

For every a, b, c, d, with $0 \leqq a < b \leqq 1$, $0 \leqq c < d \leqq 1$, the functions $\Phi(f;x;c,d)$ and $\phi(f;y;a,b)$ are defined almost everywhere, have values in the interval $[0,+\infty]$, and are measurable, and so the above integrals have meaning.

The function $f(x,y)$ is of generalized bounded variation if $\Phi_1(f)$ and $\Phi_2(f)$ are both finite; otherwise, it is of generalized unbounded variation. For continuous $f(x,y)$, our definition agrees with that of bounded variation in the sense of Tonelli, and in the general case, agrees with Cesari's definition [2] of a function of type gBVT (or of generalized variation in the sense of Tonelli).

Since, for every n, the integral mean $f_n(x,y)$ is ACT, it follows that

$$\Phi_2(f_n) = \int_0^{1-1/n}\int_0^{1-1/n} |\partial f_n/\partial y|\, dx\, dy$$

$$\text{and } \Phi_2(f_n) = \int_0^{1-1/n}\int_0^{1-1/n} |\partial f_n/\partial x|\, dx\, dy.$$

We retain the convention of convergence on the closed interval $[0,+\infty]$, and we prove

THEOREM 2. *For every summable $f(x,y)$, the integral means $f_n(x,y)$ satisfy*

$$\lim_{n\to\infty}\Phi_1(f_n) = \Phi_1(f) \text{ and } \lim_{n\to\infty}\Phi_2(f_n) = \Phi_2(f).$$

Proof. We prove the theorem for $\Phi_2(f)$. Since

$$\partial f_n(x,y)/\partial x = n^2\int_0^{1/n}\{f(x+1/n,y+v) - f(x,y+v)\}dv$$

almost everywhere, it follows that

$$\Phi_2(f_n) = \int_0^{1-1/n}\int_0^{1-1/n} n^2\left|\int_0^{1/n}\{f(x+1/n,y+v)-f(x,y+v)\}dv\right| dx\, dy$$

$$\leqq \int_0^{1-1/n}\int_0^{1-1/n} n^2\int_0^{1/n}|f(x+1/n,y+v)-f(x,y+v)|dv\, dx\, dy$$

$$= \int_0^{1-1/n} n^2\, dy\int_0^{1/n}\int_0^{1/n}\sum_{k=1}^{n-1}|f(x+k/n,y+v)-f(x+(k-1)/n,y+v)|\, dx\, dv$$

$$= n^2\int_0^{1/n}\int_0^{1/n} dx\, dv\left\{\int_0^{1-1/n}\sum_{k=1}^{n-1}|f(x+k/n,y+v)-f(x+(k-1)/n,y+v)|\, dy\right.$$

$$= n^2\int_0^{1/n} dv\int_v^{v+1-1/n} dt\int_0^{1/n}\sum_{k=1}^{n}|f(x+k/n,t)-f(x+(k-1)/n,t)|\, dx.$$

For every v and for all $t \in E_y\cdot[v,v+1-1/n]$, that is for almost all

$t \varepsilon [v, v+1-1/n]$, we have: for almost all x, the points $(x,t), (x+1/n, t)$, $\cdots, (x+(n-1/n, t)$ are all points of approximate continuity for $f(x,y)$ with respect to x, and hence:

$$\sum_{k=1}^{n} |f(x+k/n, t) - f(x+(k-1)/n, t)| \leqq \phi(f, t).$$

Then for the same v and t we have

$$\int_0^{1/n} \sum_{k=1}^{n} |f(x+k/n, t) - f(x+(k-1)/n, t)| \leqq n^{-1}\phi(f, t),$$

and finally

$$\Phi_2(f_n) \leqq n^2 \int_0^{1/n} dv \int_v^{v+1-1/n} dt \cdot n^{-1}\phi(f, t)$$

$$\leqq n^2 \int_0^1 dt \int_0^{1/n} dv \cdot n^{-1}\phi(f, t) = \int_0^1 \phi(f, t)dt = \Phi_2(f).$$

We have thus shown that $\Phi_2(f_n) \leqq \Phi_2(f)$, for every n, so that

$$\limsup_{n\to\infty} \Phi_2(f_n) \leqq \Phi_2(f).$$

It remains for us to show that $\liminf_{n\to\infty} \Phi_2(f_n) \geqq \Phi_2(f)$. For this, we need the well known fact that $f_n(x,y)$ converges almost everywhere to $f(x,y)$ so that it converges almost everywhere in each variable for almost all values of the other variable.

We suppose that $\Phi_2(f) < +\infty$ and let $\epsilon > 0$. We then have $\phi(f;y) < +\infty$ for almost all values of y, and for every such y there is $b(y) < 1$ for which

$$\phi(f;y;0,b(y)) > \phi(f;y) - \epsilon/2,$$

where $\phi(f;y) = \phi(f;y;0,1)$. It follows that there is a $b < 1$ such that,

$$\int_0^1 \phi(f;y;0,b)\,dy > \Phi_2(f) - \epsilon/2.$$

Moreover, there is $a < 1$ such that

$$\int_0^a \phi(f;y;0,b)\,dy > \Phi_2(f) - \epsilon/2.$$

Let n_1 be a positive integer such that $n_1^{-1} < \min(1-a, 1-b)$. It is easy to see, and proved in [3], that the generalized variation $\phi(f)$ of a function $f(x)$ of one variable is lower semicontinuous with respect to almost everywhere convergence. It follows that, for almost all values of y, we have

$$\liminf_{n\to\infty} \phi(f_n;y;0,b) \geqq \phi(f;y;0,b).$$

Hence, for almost every y, there is an $n(y)$ such that $n > n(y)$ implies

$$\phi(f;y;0,b) > \phi(f;y;0,b) - \epsilon/2.$$

There is then a single N, which may be taken so that $N > n_1$, such that for $n > N$,

$$\Phi_2(f_n) \geqq \int_0^{1-1/n} \phi(f_n;y;0,b)dy \geqq \int_0^{1-1/n} \phi(f;y;0,b)dy - \epsilon/2$$

$$\geqq \int_0^a \phi(f;y;0,b)dy - \epsilon/2 \geqq \Phi_2(f) - \epsilon.$$

This completes the proof for the case $\Phi_2(f) < +\infty$. The case $\Phi_2(f) = +\infty$ provides no additional difficulties, so that Theorem 2 is proved.

Now, for every n, we have the inequalities

$$\Phi_1(f_n) + \Phi_2(f_n) + 1 \geqq A(f_n) \geqq \max[\Phi_1(f_n), \Phi_2(f_n)],$$

where $A(f_n)$ is the Lebesgue area of the integral mean $f_n(x,y)$. It follows that, if $f(x,y)$ is of generalized unbounded variation, the sequence $\{A(f_n)\}$ converges to $+\infty$, so that $f(x,y)$ has the property R.

To show that $\{A(f_n)\}$ converges when $f(x,y)$ is of generalized bounded variation, we consider the generalized Geöcze expression $\Psi(f)$. A subdivision ρ of I into rectangles $R_1, R_2, \cdots, R_m$ by means of lines parallel to the coordinate axes is *admissible* if $f(x,y)$ is approximately continuous in x for almost all y on all boundary lines of the rectangles of the subdivision parallel to the y axis, and in y for almost all x on all boundary lines parallel to the x axis. The meaning of the notation $\Phi_1(f;R_i)$, $\Phi_2(f;R_i)$, $i = 1, 2, \cdots, m$, should be clear, and it follows from the essential additivity of the generalized variation function $\phi(f;a,b)$ that

$$\Phi_1(f) = \sum_{i=1}^m \Phi_1(f;R_i) \text{ and } \Phi_2(f) = \sum_{i=1}^m \Phi_2(f;R_i).$$

We then consider the expression

$$\Psi(f;\rho) = \sum_{i=1}^m \Psi(f;R_i) = \sum_{i=1}^m [\{\Phi_1(f;R_i)\}^2 + \{\Phi_2(f;R_i)\}^2 + |R_i|^2]^{\frac{1}{2}},$$

where $|R_i|$ is the area of R_i, and then let

$$\Psi(f) = \sup \Psi(f;\rho) \text{ for all admissible subdivisions } \rho.$$

Since $\Psi(f) \leqq \Phi_1(f) + \Phi_2(f) + 1$, it follows that $\Psi(f) < +\infty$. For continuous surfaces, $\Psi(f)$ is the Geöcze area so that, in particular, for the integral means of our summable $f(x,y)$, we have $\Psi(f_n) = A(f_n)$.

Again using the fact that if $f(x)$ is of bounded generalized variation, then for every $\epsilon > 0$ there is a $\delta > 0$ such that if $S \subset E$ and $\nu(S) < \delta$, then $\phi(f; S) < \phi(f) - \epsilon$, where E is the set of points of approximate continuity of $f(x)$, we obtain an alternate definition for $\Psi(f)$. Indeed, as we shall prove, $\Psi(f) = \chi(f)$, where

$$\chi(f) = \sup \chi(f; \rho) \text{ for all admissible subdivisions } \rho,$$

and

$$\chi(f; \rho) = \sum_{i=1}^{m} [\{\chi_1(f; R_i)\}^2 + \{\chi_2(f; R_i)\}^2 + |R_i|^2]^{\frac{1}{2}},$$

where

$$\chi_1(f; R_i) = \int_{c_i}^{d_i} |f(b_i, y) - f(a_i, y)|\, dy$$

$$\text{and } \chi_2(f; R_i) = \int_{a_i}^{b_i} |f(x, d_i) - f(x, c_i)|\, dx,$$

the rectangle R_i being given by $a_i \leqq x \leqq b_i$, $c_i \leqq y \leqq d_i$.

Analogously, if

$$\chi_1(f; \rho) = \sum_{i=1}^{m} \chi_1(f; R_i), \qquad \chi_2(f; \rho) = \sum_{i=1}^{m} \chi_2(f; R_i),$$

let

$$\chi_1(f) = \sup \chi_1(f; \rho), \qquad \chi_2(f) = \sup \chi_2(f; \rho)$$

for all admissible subdivisions. Obviously, we have

$$\chi_i(f) \leqq \Phi_i(f), \quad i = 1, 2, \qquad \chi(f) \leqq \Psi(f).$$

We show that $\Psi(f) = \lim_{n \to \infty} \Psi(f_n) = \lim_{n \to \infty} A(f_n)$. We first let $\epsilon > 0$ and let ρ be an admissible subdivision $R_1, R_2, \cdots, R_m$ for which $\Psi(f; \rho) > \Psi(f) - \epsilon$. By Theorem 2,

$$\liminf_{n \to \infty} \Phi_1(f_n; R_i) \geqq \Phi_1(f; R_i) \text{ and } \liminf_{n \to \infty} \Phi_2(f_n; R_i) \geqq \Phi_2(f; R_i),$$

for every $i = 1, 2, \cdots, m$, so that $\liminf_{n \to \infty} \Psi(f_n; R_i) \geqq \Psi(f; R_i)$. It follows that $\liminf_{n \to \infty} \Psi(f_n; \rho) \geqq \Psi(f; \rho) \geqq \Psi(f) - \epsilon$ and, since $\epsilon > 0$ is arbitrary. $\liminf_{n \to \infty} A(f_n) \geqq \Psi(f)$.

Conversely, $\limsup_{n \to \infty} A(f_n) \leqq \chi(f)$. In showing this, we use the expression (3) for $A(f_n)$. Then

$$A(f_n) = \int_0^{1-1/n}\int_0^{1-1/n}[1+\{n^2\int_0^{1/n}(f(x+1/n, y+v)-f(x,y+v))dv\}^2$$

$$+\{n^2\int_0^{1/n}(f(x+u, y+1/n)-f(x+u,y))du\}^2]^{\frac{1}{2}}\,dx\,dy$$

$$= n^2\int_0^{1/n}\int_0^{1/n}dx\,dy\sum_{j=1}^{n-1}\sum_{i=1}^{n-1}[n^{-4}+\{\int_0^{1/n}(f(x+\frac{i}{n}, y+\frac{(j-1)}{n}+v)$$

$$-f(x+\frac{(i-1)}{n}, y+\frac{(j-1)}{n}+v))dv\}^2$$

$$+\{\int_0^{1/n}(f(x+\frac{(i-1)}{n}+u, y+\frac{j}{n})-f(x+\frac{(i-1)}{n}+u, y+\frac{(j-1)}{n}))du\}^2]^{\frac{1}{2}}.$$

But, for almost all $(x,y)\,\varepsilon\,[0,1-1/n]\times[0,1-1/n]$, the subdivision obtained by means of the lines

$$x = x, x+1/n, \cdots, x+(n-1)/n; \qquad y = y, y+1/n, \cdots, y+(n-1)/n,$$

is admissible, so that

$$\sum_{j=1}^{n-1}\sum_{i=1}^{n-1}[n^{-4}+\{\int_0^{1/n}(f(x+\frac{i}{n}, y+\frac{(j-1)}{n}+v)$$

$$-f(x+\frac{(i-1)}{n}, y+\frac{(j-1)}{n}+v))dv\}^2$$

$$+\{\int_0^{1/n}(f(x+\frac{(i-1)}{n}+u, y+\frac{j}{n})$$

$$-f(x+\frac{(i-1)}{n}+u, y+\frac{(j-1)}{n}))du\}^2]^{\frac{1}{2}} \leqq \chi(f).$$

It then follows, since $A(f_n)$ is the mean value of the left hand side of this last inequality, that $A(f_n)\leqq\chi(f)$, for every $n=1,2,\cdots$ so that $\limsup_{n\to\infty} A(f_n)\leqq\chi(f)$. Thus we have

$$\limsup_{n\to\infty} A(f_n)\leqq\chi(f)\leqq\Psi(f)\leqq\liminf_{n\to\infty} A(f_n),$$

and hence

$$\lim_{n\to\infty} A(f_n) = \chi(f) = \Psi(f).$$

Analogously, we can prove that $\chi_1(f)=\Phi_1(f)$, $\chi_2(f)=\Phi_2(f)$. This completes the proof of

THEOREM 3. *Every summable function $f(x,y)$ has the property R.*

According to L. Cesari [2], the function $f(x,y)$ is said to be of type gBVT, or of generalized bounded variation in the sense of Tonelli, if when a

certain set of measure zero is neglected, the function is of bounded variation with respect to each variable on the remaining set for almost all values of the other variable, and these modified variation functions are both summable. As proved in [3], the summable function $f(x,y)$ is gBVT if and only if $\chi_1(f)$, $\chi_2(f)$ are both finite. The considerations above prove also that $f(x,y)$ is gBVT if and only if $\Phi_1(f)$ and $\Phi_2(f)$ are both finite.

We turn now to parametric surfaces. C. B. Morrey [4] obtained results regarding the integral means for a parametric representation $f: x_i(u,v)$, $i=1,2,3$; perhaps his main result is that if the $x_i(u,v)$ are all ACT and if each pair of partial derivatives $\partial x_i/\partial u$, $\partial x_i/\partial v$ appearing as a product in one of the jacobians belongs to conjugate L_p spaces, then the jacobians of the integral means $x_i^n(u,v)$ of $x_i(u,v)$ converge almost everywhere, and in L_1 to those of $x_i(u,v)$. In particular, it follows that f has property R. The following fact is important in this connection: If $f(x,y)$ is ACT and if $f_n(x,y)$ is the n-th integral mean of $f(x,y)$, then $\partial f_n(x,y)/\partial x$ and $\partial f_n(x,y)/\partial y$ are the n-th integral means of $\partial f(x,y)/\partial x$ and $\partial f(x,y)/\partial y$ almost everywhere. We observe that this holds for $f(x,y)$ of type gACT, but the proof is not very different from the one for the continuous case, and so it will not be given. The definition of a gACT function [3] is the same as that of an ACT function except that the continuity restriction is waived.

The following extension of Morrey's theorem holds.

THEOREM A. *A mapping $f: x_i(u,v)$, $i=1,2,3$, has property R if the $x_i(u,v)$ are gACT and one of the following conditions is satisfied:*

a) *All partial derivatives $\partial x_i/\partial u$, $\partial x_i/\partial v$, $i=1,2,3$, are in L_2.*

b) *At least two of the $x_i(u,v)$ have bounded partial derivatives and the others are integrable.*

c) *Each pair $\partial x_i/\partial u$, $\partial x_i/\partial v$ appearing as a product in one of the jacobians belongs to conjugate L_p spaces.*

It is understood that sets of measure zero may be neglected in calculating partial derivatives appearing in this theorem. The proofs are then much like the continuous case, and are omitted.

In conclusion, we wish to point out that there are mappings which do not satisfy any of the above conditions and still have property R. For example, we consider the Geöcze mapping $f: x_i(u,v)$, $i=1,2,3$. Here, let $f_1(x)$, $f_2(x)$ be a continuous mapping on $[0,1]$ whose image covers the unit square; and let $x_1(u,v)=f_1(u)$, $x_2(u,v)=f_2(u)$, $x_3(u,v)=0$. The functions $x_1(u,v)$,

$x_2(u, v)$ are not of type gACT. We observe that the integral means $x_3^n(u, v)$ are zero so that

$$A(f_n) = \int_0^{1-1/n} \int_0^{1-1/n} | \partial(x_1^n, x_2^n)/\partial(u, v) | \, du \, dv.$$

But $x_i(u, v) = x_i(u + h, v)$, $i = 1, 2$, for every u, v, h, so that

$$\int_0^{1/n} \int_0^{1/n} x_i(u + \xi, v + \eta) \, d\xi \, d\eta = \int_0^{1/n} \int_0^{1/n} x_i(u + h + \xi, v + \eta) \, d\xi \, d\eta,$$

and $x_i^n(u + h, v) = x_i^n(u, v)$. It follows that $\partial x_i^n/\partial u = 0$, $i = 1, 2$; $n = 1, 2, \cdots$; u and v arbitrary. Thus $A(f_n) = 0$, so that f has property R.

THE UNIVERSITY OF OKLAHOMA.

BIBLIOGRAPHY.

[1] T. Radó, "Sur le calcul de l'aire des surfaces courbes," *Fundamenta Mathematicae*, vol. 10 (1927), pp. 197-210.

[2] L. Cesari, "Sulle funzioni a variazione limitata," *Annali Scuola Normale Superiore Pisa*, Ser. 2, vol. 5 (1936), pp. 299-313.

[3] C. Goffman, "Lower semi-continuity and area functionals, I. The non-parametric case," *Rendiconti del Circolo Matematico di Palermo*, Ser. 2, vol. 2 (1953), pp. 203-235.

[4] C. B. Morrey, "A class of representations of manifolds," *American Journal of Mathematics*, vol. 57 (1935), pp. 275-293.

[5] T. Radó, *Length and Area*, New York, 1948.

[6] L. Cesari, *Surface Area*, Princeton, in press.

ON THE RAMIFICATION OF ALGEBRAIC FUNCTIONS.* [1]

By SHREERAM ABHYANKAR.

Introduction. The investigations of the present paper arose from our (unsuccessful) attempt to adapt the ideas of Jung's classical proof of the theorem of local uniformization on algebraic surfaces over the field of complex numbers [2] to the solution of the local uniformization problem for algebraic surfaces over fields of nonzero characteristic.[3] To explain matters, let us consider the following situation. Let T be a rational transformation from an r-dimensional normal algebraic variety V onto an r-dimensional nonsingular algebraic variety W such that T and T^{-1} are free from fundamental points. Let the ground field k be algebraically closed of characteristic p. Let P and Q be corresponding points on V and W respectively and let B be the branch locus of T^{-1} on W. Let E and F be the quotient fields of the completions of the quotient rings of P and Q on V and W respectively. Then E can be canonically considered to be a finite separable algebraic extension of F. Let E^* be a least Galois extension of F containing E. Let us denote by $G(P/Q)$ the local Galois group of P over Q, i.e., the Galois group of E^* over F.

The basic facts underlying Jung's proof, then, are that for $p=0$ and $r=2$ we have: (1) If Q is a simple point of B then $G(P/Q)$ is cyclic and P is simple for V. (2) If Q is an ordinary double point of B then $G(P/Q)$ is a direct product of two cyclic groups. We shall give algebraic proofs of (1) and (2) in Section 2, and shall show in Section 3, by examples, that these statements are no longer true if $p \neq 0$; namely we shall show that P may be a singular point of V even if Q is a simple point of B, and that the local Galois groups above simple or ordinary double points of B can be very complicated and even insolvable. The collapse of statements (1) and (2) is the reason for the nonadaptability of Jung's method of uniformization to the case

---

* Received April 6, 1955.

[1] The material of this paper together with paper [1] forms the author's Ph. D. thesis at Harvard University. The work was supported by a research project at Harvard University sponsored by the Office of Ordnance Research, U. S. Army, under Contract DA-19-020-ORD-3100.

[2] See [4]. For a simplified version of Jung's proof see [10].

[3] We have proved the theorem of local uniformization on algebraic surfaces over fields of nonzero characteristic in [1].

of ground fields of nonzero characteristic. An algebraic treatment of the main parts of Jung's proof will be given in Section 4.

Let now $p \neq 0$ and assume that B has a t-fold normal crossing at Q with $t \leqq r$ (for definition see Section 3). Let $\pi(P/Q)$ be the smallest subgroup of $G(P/Q)$ containing all the p-Sylow subgroups of $G(P/G)$. Then, as will be proved in Section 2, the factor group $G(P/Q)/\pi(P/Q)$ is a direct product of t cyclic groups. This characterization of local Galois groups above normal crosings is the main result of this paper. Also we shall include in Section 1, Zariski's own proof of his theorem about the purity of the branch locus.

My warmest thanks are due to Professor O. Zariski for his kind encouragement and valuable advice.

Notations. We shall use the following notations. For a valuation v of a field L we shall denote by R_v the valuation ring of v and by M_v the maximal ideal in R_v. We shall say that an integral domain A is normal, if A is integrally closed in its quotient field. If R is a local ring and M its maximal ideal, we shall express this by saying, "(R, M) is a local ring." If R is the quotient ring of an irreducible subvariety of an algebraic variety, we shall say that R is algebraic. If W is an irreducible subvariety of an algebraic variety V, we shall denote by $Q(W, V)$ the quotient ring of W on V and by $M(W, V)$ the maximal ideal in $Q(W, V)$. When the reference to the embedding variety V is clear we shall simply write $Q(W)$ and $M(W)$ for $Q(W, V)$ and $M(W, V)$ respectively. Unless otherwise stated, by a point we shall mean a rational point over the ground field under consideration.

1. The branch locus. The basic definitions and some preliminary results needed in the present paper were given by us in Section 2 of [1]. In this section we add a few more preliminary results.

In the following two lemmas we collect some well known facts about derived normal models. For proof of these lemmas we refer to Zariski's papers: see the remarks on pages 68-70 of [13] and the discussion of the birational case on pages 506-511 of [11].

LEMMA 1. *Let K be an r-dimensional algebraic function field over an algebraically closed ground field k, and let K^* be a finite separable extension of K. Let V and V^* be normal projective models respectively of K/k and K^*/k such that the rational transformation T from V^* onto V (determined by the embedding $K \subset K^*$ of the function fields of V and V^*) and its inverse map T^{-1} are free from fundamental points. Then:* (a) *To an irreducible*

subvariety W^* of V^* corresponds a unique irreducible subvariety W of V. Furthermore $\dim W^* = \dim W$ *and* $Q(W^*) \supset Q(W)$. (b) *To an irreducible subvariety W of V correspond a finite number of irreducible subvarieties $W^*_1, W^*_2, \cdots, W^*_s$ of V^*. Let (R, M) and (R^*_i, M^*_i) be the quotient rings of W^*_i and W respectively. Then $R^*_1, R^*_2, \cdots, R^*_s$ are exactly the local rings in K^* lying above R.*

LEMMA 2. *Given K/k, K^* and V as in Lemma* 1, *there exists V^* as in Lemma* 1. *Furthermore, V^* is unique up to a biregular transformation.*

DEFINITION 1. *We call V^* a derived normal model of V in K^*/k. Now let the notation be as in part* (b) *of Lemma* 1. *For a fixed index a, let E and E^*_a be the quotient fields of the completions of R and R^*_a respectively; and embed E canonically in E^*_a. Recall from Section* 2 *of* [1] *that:*

$$d(M^*_a : M) = [E^*_a : E], \quad g(M^*_a : M) = [(R^*_a/M^*_a) : (R/M)]_s,$$

$$i(M^*_a : M) = [(R^*_a/M^*_a) : (R/M)]_i, \quad r(M^*_a : M) = d(M^*_a : M)g(M^*_a : M)^{-1},$$

$$\bar{r}(M^*_a : M) = r(M^*_a : M)i(M^*_a : M)^{-1}.$$

Now we define:

$d(W^*_a : W) =$ *degree of W^*_a over $W = d(M^*_a : M)$;*

$g(W^*_a : W) =$ *separable residue degree of W^*_a over $W = g(M^*_a : M)$;*

$i(W^*_a : W) =$ *inseparability index of W^*_a over $W = i(M^*_a : M)$;*

$r(W^*_a : W) =$ *ramification index of W^*_a over $W = r(M^*_a : M)$;*

$\bar{r}(W^*_a : W) =$ *reduced ramification index of W^*_a over $W = \bar{r}(M^*_a : M)$.*

We shall say that W^*_a is ramified over W—or that W^*_a is ramified for the transformation T (or T^{-1})—if M^*_a is ramified over M. Also we shall say that W is a branch variety of V for the transformation T (or T^{-1}) if M is a branch ideal in R for the extension $K \subset K^*$.

Then W is a branch variety of V for the transformation T (or T^{-1}) if $r(W^*_i : W) > 1$ for some i or equivalently if $\sum_{i=1}^{s} g(W^*_i : W) < [K^* : K]$. By the *branch locus* of T or T^{-1}, denoted by $B(T)$ or $B(T^{-1})$ we shall mean the set of all (rational) points P of V/K such that P is on some irreducible subvariety of V/k which is a branch subvariety for T.

LEMMA 3. *Let K/k, K^*, V, V^* and T be as in Lemma* 1. *Then an*

irreducible subvariety W of V is a branch subvariety if and only if $W \subset B(T)$. Furthermore, $B(T)$ is a (proper) subvariety of V.

Proof. Let A be an affine coordinate ring of V and let A^* be the integral closure of A in K^*. Let us denote by $D(A^*/A)$ the ideal in A generated by all the discriminants $d(w_1, w_2, \cdots, w_n)$ over K of K-bases $(w_1, w_2, \cdots, w_n)$ of K^* which belong to A^*. Let $U \subset W$ be two irreducible proper subvarieties of V which are at finite distance for A. Then W is a branch variety of T if and only if $D(A^*/A) \subset M(W) \cap A$; see [7]. Therefore, if W is a branch variety then $D(A^*/A) \subset M(W) \cap A \subset M(U) \cap A$ and hence U is a branch variety. Again, if W is not a branch variety then $D(A^*/A) \not\subset M(W) \cap A$ and hence for some maximal ideal N in A containing $M(W) \cap A$ we must have: $D(A^*/A) \not\subset N$ (Hilbert Nullstellensatz). This proves our first assertion. To prove the second assertion let A be any affine coordinate ring of V and let A^* be the integral closure of A in K^*. Since K^*/K is separable, $D(A^*/A) \neq 0$ and hence the set of all points of $B(T)$ which are at finite distance for A, is a proper subvariety of the affine part of V given by A; i.e. "$B(T)$ is a set on a pure r-dimensional variety V/k such that if H is any hyperplane defined over k in the embedding projective space S_m/k of V then $B(T) \cap (S_m - H)$ is a proper subvariety in the affine space $S_m - H$." By induction on r, one can easily show that the assumption between quotation marks implies that $B(T)$ is a proper subvariety of V. Our second assertion can be proved also by using the concept and simple properties of symmetric products developed by Zariski in [14]. The proof, then, can be given as follows: Let P be a general point of V/k and let $P_1, P_2, \cdots, P_n$ be the n points which correspond to P for T^{-1} (taking coordinates in some fixed universal domain. Let $\tilde{P} = P_1 \circ P_2 \circ \cdots \circ P_n$ be the symmetric product of $P_1, P_2, \cdots, P_n$; and let $\tilde{T}$ be the irreducible algebraic correspondence with a general point pair $(P, \tilde{P})$ over k. Since T is a finitely valued rational transformation without fundamental points, the same is true for $\tilde{T}$; ($\tilde{T}$ is in fact birational). Hence for any point Q (with coordinates in a universal domain) of V there corresponds a unique point $\tilde{Q} = Q_1 \circ Q_2 \circ \cdots \circ Q_n$ under $\tilde{T}$ and hence the singular locus S of T is exactly the set of points on V to which correspond less than n points on V^* for T^{-1}. Therefore $B(T)$ coincides with the set of rational points of S (since k is algebraically closed), and hence $B(T)$ is a proper subvariety of V.

DEFINITION 2. *Let v be a real discrete valuation of a field K, K^* a finite separable extension of K, and v^* a K^*-extension of v. Let $M = M_v$ and $M^* = M_{v^*}$. We define:*

$d(v^*:v) = \textit{degree of } v^* \textit{ over } v = d(M^*:M)$;

$i(v^*:v) = \textit{inseparability index of } v^* \textit{ over } v = i(M^*:M)$;

$g(v^*:v) = \textit{separable residue degree of } v^* \textit{ over } v = g(M^*:M)$;

$r(v^*:v) = \textit{ramification index of } v^* \textit{ over } v = r(M^*:M)$;

$\bar{r}(v^*:v) = \textit{reduced ramification index of } v^* \textit{ over } v = \bar{r}(M^*:M)$.

Remark. In the notation of Lemma 3, let U be an irreducible $r-1$ dimensional subvariety of V and $U^*_1, U^*_2, \cdots, U^*_s$ the corresponding subvarieties of V^*. Let u and $u^*_1, u^*_2, \cdots, u^*_s$ be the real discrete valuations of K and K^* respectively such that $Q(U) = R_u$ and $Q(U^*_j) = R_{u^*_j}$. We observe that $\bar{r}(u^*_j:u) =$ reduced ramification index (in our sense) of u^*_j over $u =$ the usual ramification index (in the sense of valuation theory) of u^*_j over u. One might be tempted to define: U is a branch variety if and only if $\bar{r}(u^*_j:u) > 1$ for some j. One can easily see that with this definition the above Lemma is false, for then U may consist entirely of branch points without itself being a branch variety—this will certainly be so if $\bar{r}(u^*_j:u) = 1$ for all j and $i(u^*_j:u) > 1$ for some j; see Example 1 of Section 3 (the same example also shows that with this definition Theorem 1, which we shall prove in a moment, is false). Therefore our definition of a branch variety is the right one. Of course for characteristic zero the two definitions coincide.

LEMMA 4. *Let K/k and V be as in Lemma 1. Let W a proper irreducible subvariety of V, and P a simple point of V which lies on W. Let (o, m) and (R, M) be the respective local rings of W and P on V. Let $x_1, x_2, \cdots, x_r$ be regular parameters in R. Then $x_1, x_2, \cdots, x_r$ are separating coordinates for W, i.e., the set $(x_1, x_2, \cdots, x_r)$ satisfies the following four conditions:* (1) *$(x_1, x_2, \cdots, x_r)$ is a separating transcendence basis of K/k,* (2) *$k[x_1, x_2, \cdots, x_r] \subset o$,* (3) *$k[x_1, x_2, \cdots, x_r]$ contains a basis of m, and* (4) *o/m is a finite separable algebraic extension of*

$$k[x_1, x_2, \cdots, x_r]/(k[x_1, x_2, \cdots, x_r] \cap m).$$

Proof. Let $(\bar{R}, \bar{M})$ be the completion of (R, M). Since $\bar{R}$ is regular and since it contains a representative k of its residue field, it follows as in Section 5 of [6] that we can indentify $\bar{R}$ with $k[[x_1, x_2, \cdots, x_r]]$, and we can consider K as a subfield of $k((x_1, x_2, \cdots, x_r))$. By Prop. 1.5 of [4], $k((x_1, x_2, \cdots, x_r))$ and $k(x_1, x_2, \cdots, x_r)^{1/p}$ are linearly disjoint over $k(x_1, x_2, \cdots, x_r)$, and hence $K/k(x_1, x_2, \cdots, x_r)$ is separable.[4]

[4] p denotes the characteristic of k. We are assuming $p \neq 0$; for in case $p = 0$, $K/k(x_1, x_2, \cdots, x_r)$ is trivially separable.

Let $S = k[x_1, x_2, \cdots, x_r]$, $N = (x_1, x_2, \cdots, x_r)S$, $R_1 = S_N$, and $M_1 = NR_1$. Let $\bar{R}_1$ be the integral closure of R_1 in K. Then as in Proposition 2 of [1], $R = (\bar{R}_1)_{\bar{R}_1 \cap M}$. Let $A = S \cap m$, $o_1 = S_A$, and $m_1 = Ao_1$. Let $\bar{o}_1$ be the integral closure of o_1 in K. Then $o = (\bar{o}_1)_{\bar{o}_1 \cap m}$. By part (III), Lemma 4 of [1], $r(M : M_1) = 1$ Therefore by part (a) of Lemma 6 of [1], $r(m : m_1) = 1$. This shows that $(x_1, x_2, \cdots, x_r)$ is a separating coordinate system of W.

The following theorem and its proof are due to Professor Zariski and were communicated to me personally. The proof is based on Zariski's paper [12].

THEOREM 1. *Let K/k, K^*, V, V^* and T be as in Lemma 1. Let $B = B(T)$ be the branch locus of T on V and let $B^* = T^{-1}\{B\}$. Let W be a simple irreducible subvariety of V and W^* a corresponding subvariety of V^*.* (a) *If W^* is ramified over W, then there exists an $r-1$ dimensional irreducible subvariety U^* of V^* containing W^* such that U^* is ramified over its corresponding subvariety U of V.* (b) *The components of B^* and B passing respectively through W^* and W are pure $r-1$ dimensional.* (c) *If $B(T)$ contains no singular points of V, in particular if V is nonsingular, then $B(T)$ is pure $r-1$ dimensional.*

Proof. First observe that (b) and (c) follow at once from (a) and that in the proof of (a) we may, without loss of generality, let W^* and W be points (rational over k) P^* and P respectively. Now let (R^*, M^*) and (R, M) be the respective local rings of P^* and P, and let $(x_1, x_2, \cdots, x_r)$ be regular parameters in R. Let $(y_1, y_2, \cdots, y_m)$ be an affine general point of V^*/k for which P^* is at finite distance. Let $A = k[y_1, y_2, \cdots, y_{m+r}]$ where $y_{m+i} = x_i$ for $i = 1, 2, \cdots, r$. Then $R^* = A_{A \cap M^*}$ and hence after replacing V^* by the variety having $(y_1, y_2, \cdots, y_{m+r})$ as a general point over k we may assume that $(y_1, y_2, \cdots, y_{m+r})$ is a general point of V^*/k. Let $L = k(x_1, x_2, \cdots, x_r)$ and let v^* be the zero dimensional irreducible variety in the projective space S_m/L with general point $(y_1, y_2, \cdots, y_m)$ over L. Then $Q(v^*, S_m/L) = Q(V^*, S_{m+r}/k)$.[5] Now v^* is a simple point of S_m/L and hence $M(V^*, S_m/L)$ has a basis $(f_1, f_2, \cdots, f_m)$ of m elements. By multiplying by a suitable unit in $Q(V^*, S_m/L)$ we may assume that $f_i = F_i(y_1, y_2, \cdots, y_{m+r})$ where $F_i(Y_1, Y_2, \cdots, Y_{m+r}) \in k[Y_1, Y_2, \cdots, Y_{m+r}]$ for $i = 1, 2, \cdots, m$. By Lemma 4, K^*/L is separable and hence $J \neq 0$ at $Y_i = y_i$ $(i = 1, 2, \cdots, m + r)$ where $J = \partial(F_1, F_2, \cdots, F_m)/\partial(Y_1, Y_2, \cdots, Y_m)$.[6]

[5] See Section 2.2 of [12].

[6] See the Criterion for Uniformizing Parameters on page 27 of [12].

Suppose, if possible, that $J \neq 0$ at P^*. Then

$$\partial(F_1, F_2, \cdots, F_{m+r})/\partial(Y_1, Y_2, \cdots, Y_{m+r}) = J \neq 0$$

at P^*, where $F_{m+i} = Y_{m+i}$ for $i = 1, 2, \cdots, r$. Therefore $F_1, F_2, \cdots, F_{m+r}$ are uniformizing parameters in $Q(P^*, S_{m+r}/k)$.[6] Let

$$E = k[Y_1, Y_2, \cdots, Y_{m-r}] \cap M(V^*, S_{m+r}/k).$$

Since $R^* = Q(P^*, S_{m+r}/k)/E$ and since $F_i \varepsilon E$ for $i = m+1, m+2, \cdots, m+r$, we conclude that $M^* = (x_1, x_2, \cdots, x_r)R^*$ i.e. P^* is unramified over P, which is a contradiction. Therefore $J = 0$ at P^*, i.e. $J^* \varepsilon M^*$ where J^* is the value of J at $Y_1 = y_1$, $Y_2 = y_2, \cdots, y_{m+r} = y_{m+r}$.

Let N^* be an isolated prime ideal of J^*R^* in R^*. Since J^*R^* is principal, N^* is a minimal prime ideal in R^* and hence defines an $r-1$ dimensional subvariety U^* of V^* through P^*.[7] Let $N = N^* \cap R$ and U the subvariety defined by N. Let $S = k[x_1, x_2, \cdots, x_r]$, $D = S \cap N$. Since k is algebraically closed, S_D/DS_D is separably generated over k. By Maclane's theorem (8.2 of [12]) we can choose a separating basis from the residues of $x_1, x_2, \cdots, x_r$; say for instance $x_2, x_3, \cdots, x_r$ do this job. Fix

$$G(Y_{m+1}, Y_{m+2}, \cdots, Y_{m+r}) \varepsilon k[Y_{m+1}, Y_{m+2}, \cdots, Y_{m+r}]$$

such that $D = G(x_1, x_2, \cdots, x_r)S$. As in the proof of Lemma 4, $N = G(x_1, x_2, \cdots, x_r)R$ and $R_N/(NR_N)$ is a separable extension of $k(x_2, x_3, \cdots, x_r)$. Suppose, if possible, that N^* is unramified over N. Then $N^* = G(x_1, x_2, \cdots, x_r)R^*$ and $R^*_{N^*}/(N^*R^*_{N^*})$ is a separable extension of $k(x_2, x_3, \cdots, x_r)$. Therefore $F_1(Y_1, Y_2, \cdots, Y_{m+r})$, $F_2(Y_1, Y_2, \cdots, Y_{m+r})$, $\cdots, F_m(Y_1, Y_2, \cdots, Y_{m+r})$, $G(Y_{m+1}, Y_{m+2}, \cdots, Y_{m+r})$ are regular parameters in $Q(U^*, S_{m+r}/k)$; (see corollary on page 9 of [12]). Therefore considering G as a point in $S_{m+1}/k(x_1, x_2, \cdots, x_{r-1})$, we have:

$$\partial(F_1, F_2, \cdots, F_m, G)/\partial(Y_1, Y_2, \cdots, Y_{m+1}) = J\frac{\partial G}{\partial Y_{m+1}} \neq 0$$

at $Y_1 = y_1$, $Y_2 = y_2, \cdots, Y_{m+r} = y_{m+r}$.[6] Therefore $J \neq 0$ at $Y_1 = y_1, Y_2 = y_2, \cdots, Y_{m+r} = y_{m+r}$, which is a contradiction. Therefore U^* is ramified over U.[8]

PROPOSITION 1. *Let (R, M) be a normal algebraic local ring with quotient field K. Let K' be a finite separable extension of K and let K^* be a least Galois extension of K containing K'. Then M is a branch ideal (in R) for the extension K'/K if and only if it is so for the extension K^*/K.*

[7] R^* being normal all the primes of J^*R^* are minimal.

[8] $J = 0$ is a local equation of the component of B^* through P^*.

Proof. If M is not a branch ideal for K^*/K then by Lemma 4 of [1] it follows that M is not a branch ideal for K'/K. Now assume that M is not a branch ideal for K'/K. Let (R^*_j, M^*_j) for $j=1,2,\cdots,t$ be the local rings in K^* lying above R. Let G be the Galois group of K^*/K, G' the Galois group of K^*/K', and G_j the inertia group of M_j over M. Then by Lemma 5.V.1 of [1], $G' \supset G_j$ for $j=1,2,\cdots,t$. Let $\bar{G}$ be the smallest subgroup of G which contains $G_1, G_2, \cdots, G_t$. Then $\bar{G}$ is a normal subgroup of G and $\bar{G} \subset G'$. Therefore the fixed field $\bar{K}$ of $\bar{G}$ is a Galois extension of K containing K', and hence $\bar{K}=K^*$, i.e., $\bar{G}=(1)$. Therefore $G_1=G_2=\cdots=G_t=(1)$, and hence by Lemma 5.I.3 of [1], $r(M^*_j : M)=1$ for $j=1,2,\cdots,t$; i.e., M is not a branch ideal for K^*/K.

2. Local Galois groups.

DEFINITION 3. *Let G be a finite group, p a prime number and s an integer. Let π be the smallest subgroup of G which contains all the Sylow p-groups of G. If G is an abelian group which can be expressed as a direct product of t cyclic subgroups with $t \leqq s$, then we shall say that G is a 0_s-group. If G/π is a 0_s-group, we shall say that G is a p_s-group.*

DEFINITION 4. *Let (R, M) be the local ring of a simple point P of an r dimensional algebraic variety V, and let W be a pure $r-1$ dimensional subvariety of V. Let $W_1, W_2, \cdots, W_s$ be the irreducible components of W which pass through P. Let $N_i = R \cap M(W_i, V)$. Let s be an integer with $s \leqq r$. Then we shall say that W has an s-fold normal crossing at P if there exists a minimal basis $(x_1, x_2, \cdots, x_r)$ of M such that $x_i R = N_i$ for $i=1,2,\cdots,s$.*

LEMMA 5. *Let $R=k[[X_1, X_2, \cdots, X_r]]$, $E=k((X_1, X_2, \cdots, X_r))$, and E^* the root field of $f(Z)=Z^n-X$ over E, where in case of nonzero characteristic we assume that n is not divisible by the characteristic. Let R^* be the integral closure of R in E^*, and let X^* be a root of $f(Z)$ in E^*. Then $R^*=\sum_{i=0}^{n-1} X^{*i}R$, R^* is a regular local ring of dimension r and $(X^*, X_2, X_3, \cdots, X_r)$ are regular parameters in R^*.*

Proof. Let v be the valuation of E such that $R_v = R_{(X_1 R)}$, and let v^* be a E^*-extension of v. Since $nv^*(X^*)=v(X_1)$, v^* is the only extension of v to E^*. Since X_1^{n-1} is the discriminant of $f(Z)$, we have that: $R^*=\sum_{i=0}^{n-1}(X^{*i}X_1^{1-n})R$, (see page 79 of [9]). $u^* \varepsilon R^*$ implies that $u^*=\sum_{i=0}^{n-1} X^{*i}X_1^{1-n}u_i$ with $u_i \varepsilon R$, and $v^*(u^*) \geqq 0$. The v^* values of any two

different nonzero terms in the above sum are distinct. Hence $u_i \neq 0$ implies that $v^*(X^{*i}X_1^{1-n}u_i) \geqq 0$ and hence that $X_1^{1-n}u_i \in R$. Therefore $R^* = \sum_{i=0}^{n} X^{*i}R$. The remaining part of the lemma follows at once from this.

In the rest of this section we shall deal with the following situation. Let K be an r dimensional function field over an algebraically closed ground field k of characteristic p and let K^* be a finite separable extension of K. Let V be a projective normal model of K/k, V^* a derived normal model of V in K^*, and T the rational transformation from V^* onto V. Let P and P^* be corresponding points of V and V^*, and let (R, M) and (R^*, M^*) be the local rings of P and P^* respectively. Let Ω be an algebraic closure of K^*.

LEMMA 6. *Assume K^*/K is Galois and let $y_1, y_2, \cdots, y_h$ be a finite number of elements in R such that $N_j = y_jR$ is a minimal prime ideal in R and hence that R_{N_j} is the valuation ring a real discrete valuation w_j of K. Let n_j be the reduced ramification index over w_j of a K^*-extension of w_j.*[9] *Assume that if $p \neq 0$ then $n_j \not\equiv 0(p)$ for $j = 1, 2, \cdots, h$. Let y_j^{1/n_j} be an n_j-th root of y_j in Ω. Let*

$$\bar{K} = K(y_1^{1/n_1}, y_2^{1/n^2}, \cdots, y_h^{1/n_h}) \text{ and } \bar{K}^* = K^*(y_1^{1/n_1}, y_2^{1/n_2}, \cdots, y_h^{1/n_h}).$$

Let N_0 be a minimal prime of R different from $N_1, N_2, \cdots, N_h$ and let w_0 be the valuation of K with valuation ring R_{N_0}. Let $\bar{w}^*_j$ be an extension of w_j to $\bar{K}^*$, w^*_j the K^*-restriction of $\bar{w}^*_j$, and $\bar{w}_j$ the $\bar{K}$-restriction of $\bar{w}^*_j$. Then: (a) *$\bar{K}^*/K$, $\bar{K}/K$, $\bar{K}^*/K^*$ and $\bar{K}^*/\bar{K}$ are Galois extensions.* (b) *$r(\bar{w}^*_j : w^*_j) = \bar{r}(\bar{w}^*_j : w^*_j) = 1$ and $r(\bar{w}_j = w_j) = \bar{r}(\bar{w}_j : w_j) = n_j$ for $j = 1, 2, \cdots, h$.* (c) *$r(\bar{w}^*_0 : w^*_0) = r(\bar{w}_0 : w_0) = 1$, $r(\bar{w}^*_0 : \bar{w}_0) = r(w^*_0 : w_0)$, and $\bar{r}(\bar{w}^*_0 : \bar{w}_0) = \bar{r}(w^*_0 : w_0)$.*

Proof. We shall assume that $h = 1$, since the general case follows from this by a straightforward induction. (a) follows from the fact that the compositum of two Galois extensions of K is again a Galois extension of K. Now let $[\bar{K}^* : K^*] = n$. Then $n_1 \equiv 0(n)$. Let $x = y_1^{1/n_1}$ and $z = x^n$. Then $f(X) = X^n - z$ is the minimal monic polynomial of x over K^*. Now z^{n-1} is the discriminant of $f(X)$. Since z^{n-1} is a unit in $R_{w^*_0}$, $r(\bar{w}^*_0 : w^*_0) = 1$. Fix $u \in R_{w^*_1}$ such that $uR_{w^*_1} = M_{w^*_1}$. Then x/u is a primitive element of $\bar{K}^*/K^*$, and $g(X) = X^n - zu^{-n}$ is the minimal monic polynomial of x/u over K^*. Since $w^*_1(zu^{-n}) = 0$, the w^*_1-residue e of zu^{-n} is a nonzero element. Hence the discriminant of $X^n - e$ is also a nonzero element of $R_{w^*_1}/M_{w^*_1}$.

[9] Since K^*/K is Galois, n_j depends only on w_j.

Therefore the discriminant of $g(X)$ is a unit in $R_{w^*_1}$, and hence $r(\bar{w}^*_1 : w^*_1) = 1$. Since $n_1 \bar{w}_1(x) = w_1(y_1)$, we have that $r(\bar{w}_1 : w_1) = \bar{r}(\bar{w}_1 : w_1) = n_1$. The rest of the assertions follow in a similar fashion.

LEMMA 7. *Assume that P is simple; P^* is the only point which corresponds to P; $Z^n - x_1$ is the minimal equation of a primitive element x^* of K^*/K; $[K^* : K] \not\equiv 0$ if $p \not\equiv 0$, and that x_1 is part of a minimal basis $(x_1, x_2, \cdots, x_r)$ of M. Then P^* is simple and $M^* = (x^*, x_2, x_3, \cdots, x_r)R^*$.*

Proof. Follows from Proposition 1 of [1] and Lemma 5.

THEOREM 2. *Let $\bar{B}$ be the branch locus on V. Assume that P is simple and that the component B of $\bar{B}$, which is ramified for the extension $P \to P^*$, has a t-fold normal crossing at P.*[10] *Then the local Galois group $G(P^*/P)$ is a p_t-group.*

Proof. Let K' be the least Galois extension of K such that $K^* \subset K' \subset \Omega$, P' a point corresponding to P^* on a derived normal model of V^* in K', and (R', M') the local ring of P'. Let K_s and K^*_s be the splitting fields of P' over P and P^* respectively, and let $\bar{K}'$ be the least Galois extension of K_s such that $K^*_s \subset \bar{K}' \subset K'$. Let P_s, P^*_s, $\bar{P}'$ be the points corresponding to P' on derived normal models V_s, V^*_s, $\bar{V}'$ of V in K_s, K^*_s, $\bar{K}'$ respectively. The results of Section 1 and of Section 2 of [1] imply the following: P_s is simple; if B_s is the image of B for the transformation $V \to V_s$, then B_s is the branch variety for the extension $P \to \bar{P}'$, B_s has a t-fold normal crossing at P_s; and $G(P'/P_s) = G(P^*/P)$. Therefore we may replace V, P, V^*, P^* by V_s, P_s $\bar{V}'$, $\bar{P}'$ respectively.

Hence to start with we may assume that P^* is the only point corresponding to P and that K^*/K is Galois. Let G be the Galois group of K^*/K and let π be the smallest subgroup of G which contains all the p-Sylow groups of G if $p \not\equiv 0$ and let $\pi = (1)$ if $p = 0$. Let $\tilde{K}$ be the fixed field of π, $\tilde{V}$ a derived normal model of V in $\tilde{K}$ and P the point in $\tilde{V}$ corresponding to P^*. Then the branch locus $\tilde{B}$ for the extension $P \to P$ is a subvariety of B and hence $\tilde{B}$ has a m-fold normal crossing at P with $m \leqq t$. We have to show that G/π is a 0_t-group, and hence enough to show that G/π is a 0_m-group.

Therefore to start with we may assume that if $p \not\equiv 0$ then $[K^* : K] \not\equiv 0(p)$; and then we have to show that G is a 0_t-group. Let $(x_1, x_2, \cdots, x_r)$ be regular parameters in R such that $R_{(x_j R)} = Q(B_j, V)$ for $j = 1, 2, \cdots, t$ where

[10] By Theorem 1, $\bar{B}$ is pure $r-1$ dimensional. B consists of those irreducible components B_j of $\bar{B}$ passing through P for which there exists a corresponding variety B^*_j through P^* with $r(B^*_j : B_j) > 1$.

$B_1, B_2, \cdots, B_t$ are the irreducible components of B. Let B^*_j be an irreducible subvariety of V^* corresponding to B_j, and let $n_j = r(B^*_j : B_j)$.[11] Let x_j^{1/n_j} be an n_j-th root of x_j in Ω. Let $K_2 = K^*(x_1^{1/n_1}, x_2^{1/n_2}, \cdots, x_t^{1/n_t})$ and $K_1 = K(x_1^{1/n_1}, x_2^{1/n_2}, \cdots, x_t^{1/n_t})$. Let P_2 be a point corresponding to P^* on a derived normal model V_2 of V in K_2 and let P_1 be the point corresponding to P_2 on a derived normal model V_1 of V in K_1. Let (R_1, M_1) be the quotient ring of P_1. Theorem 1 and Lemmas 6 and 7 imply that P_1 is a simple point, $M_1 = (x_1^{1/n_1}, x_2^{1/n_2}, \cdots, x_t^{1/n_t}, x_{t+1}, x_{t+2}, \cdots, x_r)$, $G(P_2 : P) = G(P_1 : P) =$ the direct product of t cyclic groups of orders $n_1, n_2, \cdots, n_t$. Since $G(P^* : P)$ is a subgroup of $G(P_2 : P)$, we conclude that $G(P^* : P)$ is 0_t-group.

THEOREM 3.[12] *Let the assumptions be as in Theorem 2 and let $p = 0$. Let $(x_1, x_2, \cdots, x_r)$ be regular parameters in R such that $R_{(x_j R)} = Q(B_j, V)$ for $j = 1, 2, \cdots, t$; where $B_1, B_2, \cdots, B_t$ are the irreducible components of B. Let $\bar{R} = k[[x_1, x_2, \cdots, x_r]]$ and $\bar{R}^*$ be the completions of R and R^* respectively; and embed $\bar{R}$ in $\bar{R}^*$ canonically. Let E and E^* be the respective quotient fields of $\bar{R}$ and $\bar{R}^*$. Then P^* is Galois over P, $G(P^* : P)$ is a 0_t-group and $E^* \subset k((x_1^{1/n_1}, x_2^{1/n_2}, \cdots, x_t^{1/n_t}, x_{t+1}, x_{t+2}, \cdots, x_r))$ where $n_1, n_2, \cdots, n_t$ are suitable integers.*

Proof. Follows from the considerations made in the proof of Theorem 2.

THEOREM 4. *Let the assumptions be as in Theorem 3 and let $t = 1$, i.e., let B have a simple point at P. Then P^* is simple,*

$$\bar{R}^* = k[[x_1^{1/n_1}, x_2, \cdots, x_r]],$$

and $x_1 R^*$ is primary, i.e., B does not split locally for the extension $P \to P^*$.

Proof. That P^* is simple and $R^* = k[[x_1^{1/n_1}, x_2, x_3, \cdots, x_r]]$ follows from Theorem 3. Since x_1 is the power of an irreducible element in $\bar{R}^*$, it must already be so in R^*.

Remark. Let $G(P^* : P)$ be the local Galois group over a t-fold normal crossing as referred to in Theorem 2. If $p \neq 0$, $G(P^* : P)$ can be very messy and insolvable even for $t = 2$ and $t = 1$ as will be shown by Examples 3 and 4 in Section 3. Hence in a certain sense, Theorem 2 gives a best possible description of local Galois groups over normal crossings. Since

[11] $r = \bar{r}$ since $[K^* : K] \not\equiv 0 (p)$ if $p \neq 0$.

[12] Known in the classical case when k is the field of complex numbers; the known proofs being topological.

Theorem 4 essentially depends on the fact that for $p=0$ the local Galois group above a simple point of the branch locus is cyclic and since for $p\neq 0$ such a local Galois group need not be cyclic, we cannot expect this theorem to hold for $p\neq 0$. Examples 1, 2 and 5 of Section 3 will show that for $p\neq 0$, a point above a simple point of the branch locus need not be simple. Example 5 will also show that even if the branch locus B for $P\to P^*$ has a simple point at P, still the image B^* of B may split at P^*. If we have a sequence $P\to P^*_1\to P^*_2\to\cdots\to P^*_q$ such that the branch locus B for $P\to P^*_q$ has a simple point at P, B may acquire a singularity at P^*_1, and hence a bad singularity at P^*_2, and a worse one at P^*_3 etc.; thus making the groups $G(P^*_i : P^*_{i-1})$ more and more complex. This "local splitting of a simple branch variety by itself" is the real reason behind the failure of Theorem 3 and 4 for $p\neq 0$, and which in turn explains the failure for nonzero characteristic fields of Jung's classical method of uniformization (see Section 4).

3. Some examples. In the following examples we shall be dealing with a normal surface $\bar{F}$ in a projective space S_3 over algebraically closed ground field k of characteristic $p\neq 0$. $\bar{F}$ will be given by its defining homogeneous polynomial F in the homogeneous coordinates X, Y, Z, T in S_3. We shall project $\bar{F}$ from the point $X=Y=T=0$ onto the (X,Y,T) plane. By $\bar{K}$ and K we shall denote the function fields of the (X,Y,T) plane and of $\bar{F}$ respectively. By D we shall denote the branch curve of this projection on the (X,Y,T) plane. We shall omit some details in the proofs which consist of straightforward computations. For instance: since k is algebraically closed, $F=\partial F/\partial Z=\partial F/\partial X=\partial F/\partial Y=\partial F/\partial T=0$ will give the singular manifold of F (Theorem 7 of [12]). In Examples 1 to 5, F will have only a finite number of singular points, from which will follow the irreducibility of F and hence of $\bar{F}$. Consequently in Examples 1 to 5, we shall have that the singularities of F are exactly the singularities of $\bar{F}$ and the finitenes of their number will in turn imply the (arithmetic) normality of $\bar{F}$ (Theorem 3 of [8]). We shall find D by computing the Z-discriminant of F. Also we shall use well-known facts from ramification theory of real discrete valuations, for which we refer to [3] and [5].

Example 1.

$$F=\begin{cases} Z^p-X^{p-1}Z-Y^{p-1}T & \text{if } p\neq 2\\ Z^2-XZ-Y^2 & \text{if } p=2.\end{cases}$$

$\bar{F}: F=0$ is a normal surface with $X=Y=Z=0$ as the only singular point. $X=0$ is the equation of the branch curve D. *Thus* $X=Y=0$ *is a simple*

point of D and above it lies the singular point $X=Y=Z=0$ of $\bar{F}$. $\bar{K}/K$ is a cyclic extension of degree p. Consider the real discrete valuation v_X of K/k given by the Y-axis: $X=0$, in the (X,Y)-plane. For $p\neq 2$, reducing F modulo v_X we get: $Z^p - Y^{p-1}=0$. This is an irreducible pure inseparable equation over the residue field $k(Y)$ of v_X. Hence v_X has a unique extension $\bar{v}_X$ to $\bar{K}$. We have: $i(\bar{v}_X : v_X)=p$ and $\bar{r}(\bar{v}_X : v_X)=1$. For $p=2$, writing Z^* for $Z+Y$ we get: $F=Z^{*2}+XZ^*+XY$. Again v_X has a unique $\bar{v}_X$ to $\bar{K}$, but now $\bar{r}(\bar{v}_X : v_X)=2$ and $i(\bar{v}_X : v_X)=1$ since $\bar{v}_X(Z^*)=\frac{1}{2}v_X(X)$.

Example 2.

$$F=Z^p - X^{p-1}Z - XY^{p-1}.$$

$\bar{F}: F=0$ is a normal surface with $X=Y=Z=0$ as the only singuarity. $X=0$ is the equation of the branch curve D. Again *$X=Y=0$ is a simple point of D and above it lies the singular point $X=Y=Z=0$ of $\bar{F}$.* Again $\bar{K}/K$ is cyclic of degree p. Let v_X be the valuation of K/k given by $X=0$ and let $\bar{v}_X$ be an extension of v_X to $\bar{K}$. Then $\bar{v}_X(Z)=(1/p)v_X(X)$. Hence $\bar{v}_X$ is unique, $\bar{r}(\bar{v}_X : v_X)=p$, and $i(\bar{v}_X : v_X)=1$. (Note that Examples 1 and 2 coincide for $p=2$).

Example 3. $p=2$.

$$F=Z^5+XZ^2T^2+YZT^3+X^4T.$$

$\bar{F}: F=0$ is a normal surface with $X=Y=Z=0$ and $X=T=Z=0$ as the only singular points. Components of the branch curve D through the point $Q: X=Y=0$ are $X=0$ and $X^6+Y=0$. *So Q is an ordinary double point of D.*

The point $P: X=Y=Z=0$ is the only point of $\bar{F}$ above Q. Let $\bar{R}$ and R be the completions of the local rings of P and Q respectively, and let $\bar{E}$ and E be the respective quotient fields of $\bar{R}$ and E. It is clear that $R=k[[X,Y]], E=k((X,Y))$, and that

$$F(Z)=Z^5+XZ^2+YZ+X^4$$

is the minimal polynomials of a primitive element of $\bar{E}$ over E. Let E^* be the least normal extension of E containing $\bar{E}$, and let G be the Galois group of E^* over E.

We shall show that G is insolvable.

Since E^*/E is the root field of $f(Z)=0$ we can consider G as a subgroup of the permutation group P_5 on five symbols. Let n be the order of G.

Consider the discrete valuation v_X of $\bar{E}$ given by the prime element X of R. Reducing the equation $f(Z)=0$ modulo v_X we get:

$$Z^5+YZ=Z(Z^4+Y)=0.$$

Therefore there exists a valuation of E^* above v_X with inseparability index divisible by 4.

Similarly reducing $f(Z)=0$ module the valuation v_{Y-X^6} of E given by $Y-X^6$ we get:

$$Z^5+XZ^2+X^6Z+X^4=(Z^2+X^3)(Z^3+X^3Z+X)=0.$$

Therefore there exists a valuation of E^* above v_{X-Y^6} with residue degree divisible by 3.

Hence n is divisible by 3, 4 and 5; i.e., n is divisible by 60. Since P_5 is of order 120 and since the alternating group A_5 is the only subgroup of P_5 of order 60; it follows that G is either A_5 or P_5. In either case G is insolvable.

Example 4. $p=2$.

$$F=Z^5+XZ^4+YZ^3T+X^4Z+XY^2T.$$

Again $\bar{F}:F=0$ is a normal surface with $X=Y=Z=0$ and $X=T=Z=0$ as the only singular points. But now $X=0$ is the only component of D through the point $Q:X=Y=Z=0$. *So Q is a simple point of D.* Also $P:X=Y=Z=0$ is the only point of F above Q. Let R, $\bar{R}$, E, $\bar{E}$, E^* and G be as Example 3. Now $f(Z)=Z^5+XZ^4+YZ^3+X^4Z+XY^2$ is the minimal polynomial of a primitive element of $\bar{E}/E$. Again consider G as a subgroup of the permutation group P_5 on five symbols.

Reducing $f(Z)=0$ module the valuation v_X of E given by the prime element X of R we get:

$$Z^3(Z^2+Y)=0.$$

Therefore there exists a valuation v_1 of $\bar{E}$ above v_X with inseparability index divisible by 2. Also we have that there is an extension v_2 of v_X to $\bar{E}$ such that $v_2(z)>0$ where z is a root of $f(Z)=0$. It is clear that Yz^3 and XY^2 must be the minimum value terms in $f(z)$ for v_2, i.e., we have $v_2(Yz^3)=v_2(XY^2)$. Since $v_2(Y)=v_X(Y)=0$ and $v_2(X)=v_X(X)=1$; it follows that $v_2(z)=\frac{1}{3}$, and hence we have that $\bar{r}(v_2:v_X)\geqq 3$. Now $v_1=v_2$ implies that $r(v_1:v_X)\geqq 6>[\bar{E}:E]$ which is a contradiction. Hence $v_1\neq v_2$. Therefore $i(v_1:v_X)+\bar{r}(v_2:v_X)\leqq 5=[\bar{E}:E]$ i.e., $\bar{r}(v_2:v_X)=3$. Therefore every extension v^* of v_X to E^* is such that $i(v^*:v_X)$ is divisible by 2 and $\bar{r}(v^*:v_X)$ is divisible by 3.

Therefore the order n of G is divisible by 2, 3, 5 and hence by 30. Hence G is either (i) P_5, or (ii) A_5, or (iii) a subgroup of P_5 of order 30. In cases (i) and (ii) G is insolvable. We shall show that case (iii) cannot arise by proving that P_5 *has no subgroup of order* 30. Suppose then, if possible, that H is a subgroup of P_5 of order 30. Let $H = H_1, H_2, H_3, H_4$ be the right cosets of H, and for $u \in P_5$ let

$$(tu)(H_1, H_2, H_3, H_4) = (H_1u, H_2u, H_3u, H_4u).$$

Then t is a homomorphism of P_5 into the group of permutations of H_1, H_2, H_3, H_4. Since $u \in H_i$ implies $H_1u = H_i$, $4 \leqq$ order of $t(P_5) \leqq 24$. Hence $t^{-1}(0)$ is a normal subgroup of P_5 of order m, where $(120)/(24) = 5 \leqq m \leqq 30 = 120/4$. A contradiction since A_5 is the only normal subgroup of P_5. *Therefore G is insolvable.*

Example 5.

$$F = Z^{p+1} + Y^{p-1}ZT + X^{p+1}.$$

The surface $\bar{F}: F = 0$ is normal and has $X = Y = Z = 0$ and $X = T = Z = 0$ as the only singular point. *The point $Q: X = Y = 0$ is a simple point of the branch curve $D: X = 0$.* Again in the terminology of Example 3,

$$f(Z) = Z^{p+1} + Y^{p-1}Z + X^{p+1},$$

is the minimal polynomial of a primitive element of $\bar{E}/E$. Consider the Galois group G of E^*/E, as a subgroup of the permutation group P_{p+1} on the roots of $f(Z) = 0$. Modulo the valuation v_X of E given by the prime element X in R the equation $f(Z) = 0$ becomes $Z(Z^p + Y^{p-1}) = 0$. Hence there exists a valuation of E^* above v_X with inseparability index divisible by p. Since the order n of G must then be divisible by p and since p is prime, G must contain a p-cycle. Thus G is a subgroup of P_{p+1}, G contains a p-cycle, and the order of G is divisible by $p(p+1)$. For $p \geqq 5$ such a group G is very large and quite complicated.

Observe that *the point $P = X = Y = Z = 0$ is above the simple point $Q: X = Y = 0$ of the branch curve $D: X = 0$*; and still *P is singular. D splits in passing from Q to P* as is shown by the equation: $Z(Z^p + Y^{p-1}) = 0$.

Example 6. $p = 5$.

$$F = Z^5 + YZ^3 + YZ^2 + X.$$

$\bar{F}: F = 0$ is nonsingular at finite distance. *$Q: X: Y = 0$ is an ordinary double point of the local branch curve $XY = 0$.* The only point of $\bar{F}$ above Q is

$P: X = Y = Z = 0$. *P is a simple point of $\bar{F}$ but still the local Galois group G of P over Q* (notation of Example 3) *is insolvable.*

Modulo the valuation v_X of E given by X, we have

$$Z^5 + YZ^3 + YZ^2 = Z^2(Z^3 + YZ + Y) = 0.$$

Hence there exists a valuation v_1 of $\bar{E}$ over v_X with separable residue degree over v_X divisible by 3. Also there is a valuation v_2 of $\bar{E}$ above v_X for which $v_2(z) > 0$ where z is a root of $F(Z) = 0$. Since for v_2, Yz^2 and X are the minimum value terms of $F(z)$; it follows that $v_2(z) = (\frac{1}{2})v_X(X) = \frac{1}{2}$. As in Example 4 we conclude that: $v_1 \neq v_2$, $\bar{r}(v_2 : v_X) = 2$, and $g(v_1 : v_X) = 3$. (One extension with $g = 3$ and one extension with $\bar{r} = 2$ makes up $3 + 2 = 5 = [\bar{E} : E]$ and accounts for all the $\bar{E}$-extensions of v_X). Hence the order of G is divisible by $2 \times 3 \times 5 = 30$. The insolvability of G now follows as in Example 4.

Remark. In the above examples, let Q and P be the points $X = Y = 0$ and $X = Y = Z = 0$ of the (X, Y, T) plane and of $\bar{F}$ respectively. Observe that in all the examples: $r(P : Q) = \bar{r}(P : Q) = [\bar{K} : K] = [\bar{E} : E]$. Now let K^* be the least Galois extension of K containing $\bar{K}$, and let P^* be a point corresponding to P on a derived normal model F^* of the (X, Y, T) plane in K^*. By Proposition 1, D is the branch curve also for the rational transformation from F^* onto the (X, Y, T) plane. In Example 3, Q is an ordinary double point of D and in Examples 4 and 5, Q is a simple point of D. In Examples 3 and 4, $G(P^* : Q)$ is insolvable. In Example 5, since D splits in passing from Q to P, D splits *a fortiori* in passing from Q to P^*. In Examples 1 and 2, $\bar{K} = K^*$ and hence $P = P^*$.

4. Jung's method of uniformization. Let S be an algebraic surface in an n-dimensional projective space over an algebraically closed ground field k and let K be the function field of S. The classical problem of local uniformization on algebraic surfaces deals with the case when k is the field of complex numbers. It roughly asserts the following: Let P be a point on S. Then some complete neighborhood of P on S can be covered by a finite number of regions $R_1, R_2, \cdots, R_t$ such that in each R_i the coordinates $x_1, x_2, \cdots, x_n$ of the points in R_i can be expressed as convergent power series in two variables u, v; this representation being unramified in a certain sense. This problem was solved by Jung[2] by using a very fruitful method. Zariski generalized this problem when k is an abstract field, stating it in terms of valuation theory. If we use the concept of normal varieties due to Zariski,

then the basic ideas behind Jung's proof become strikingly simple and are as described below.

Let V be a normal model of the function field K/k in a projective space S_r or dimension r. Project V onto a plane V', from an S_{r-3} which does not meet V. Let K'/k be the function field of V'. Let T be the rational transformation from V onto V', thus defined. Since T and T^{-1} are free from fundamental points, V is a derived normal model of V' in K. By Theorem 2, the branch locus D on V is a curve. Let Q be a singular point of D. Apply to V' a locally quadratic transformation t, with center Q, getting a new surface V'_1. To Q there will correspond a fundamental line L_1 on V'_1. We have that there is a rational transformation tT of V onto V'_1 whose inverse is finitely valued at each point of V'_1. Let V_1 denote a derived normal model of V'_1 in the function field K/k. Let T_1 be the rational transformation of V_1 onto V'_1 (defined in a natural fashion). Then V_1, V'_1 and T_1 are in the same relationship to each other as V, V' and T. Also V_1 has no singular points. The branch curve D_1 of T_1^{-1} is either the proper transform of D, or it is this transform together with the line L_1. After a finite number of steps it is possible to get V_1, V'_1 and T_1 such that the branch curve D_1 on V'_1 has only ordinary double points. We may assume that already V, V', and T have this property, i.e., that D has only ordinary double points.

Let Q be a point of V' and let P be a point of V corresponding to Q. We have proved in Section 2 that: (a) If $Q \notin D$, then P is a simple point of V. (b) If Q is a simple point of D, then $G(P/Q)$ is cyclic and again P is a simple point. (c) If Q is an ordinary double point of D, then $G(P/Q)$ is the direct product of two cyclic groups.[12] So it is only necessary to consider what happens "above" an ordinary double point Q of the branch curve D. Let P be a point of V above Q. The simple structure of $G(P/Q)$ in this case enables Jung to resolve the singularity of V at Q in the classical case when k is the field of complex numbers, by topological considerations.

Now supposing that k is of characteristic $p \neq 0$, we tried to generalize Jung's method. But unfortunately in this case of modular ground fields as was shown in Section 3, the statements (b) and (c) are not valid and the groups mentioned there may even be insolvable. If these local Galois groups were at least solvable, that would have been of some use for the purposes of uniformization.

HARVARD UNIVERSITY.

BIBLIOGRAPHY.

[1] S. Abhyankar, "Local uniformization on algebraic surfaces over ground fields of characteristic $p \neq 0$," forthcoming in the *Annals of Mathematics*.

[2] C. Chevalley, "Some properties of ideals in rings of power series," *Transactions of the American Mathematical Society*, vol. 55 (1944), pp. 68-84.

[3] M. Deuring, "Verzweigungstheorie bewerteter Körper," *Mathematische Annalen*, vol. 105 (1931), pp. 277-307.

[4] H. W. E. Jung, "Darstellung der Funktionen eines algebraischen Körpers zweier unabhängigen Veränderlichen in der Umgebung einer Stelle," *Journal Für Mathematik*, vol. 133 (1908), pp. 289-314.

[5] W. Krull, "Galoissche Theorie bewerteter Körper," *Sitzungbereichte der Bayerschen Akad. der Wissenschaften*, München (1930).

[6] ———, "Dimensionstheorie in Stellenringe," *Journal Für Mathematik*, vol. 179 (1938), pp. 204-226.

[7] ———, "Der allgemeine Diskriminantensatz," *Mathematische Zeitschrift*, vol. 45 (1939), pp. 1-19.

[8] A. Seidenberg, "The hyperplane sections of normal varieties," *Transactions of the American Mathematical Society*, vol. 69 (1950), pp. 357-383.

[9] B. L. van der Waerden, *Modern Algebra*, Vol. II, New York, 1950.

[10] R. J. Walker, "Reduction of the singularities of an algebraic surface," *Annals of Mathematics*, vol. 36 (1935), pp. 336-365.

[11] O. Zariski, "Foundations of a general theory of birational correspondences," *Transactions of the American Mathematical Society*, vol. 53 (1943), pp. 490-542.

[12] ———, "The concept of a simple point of an abstract algebraic variety," *ibid.*, vol. 62 (1947), pp. 1-52.

[13] ———, *Theory and Applications of Holomorphic Functions on Algebraic Varities over Arbitrary Ground Fields*, New York, 1951.

[14] ———, "Abstract Algebraic Geometry, Vol. I," forthcoming in the *American Mathematical Society* Publications.

A NOTE ON TWO DIMENSIONAL DIVISION RING EXTENSIONS.*[1]

By N. JACOBSON.

A division subring Γ of a division ring Δ is said to be *Galois in* Δ (and Δ is *Galois over* Γ) if Γ is the set of invariants (or fixed points) of a group of automorphisms acting in Δ. The two dimensional Galois extensions of a division ring have been determined by Dieudonné.[2] In this note we shall show that if Γ is a division ring of characteristic $\neq 2$ which is finite dimensional over its center Ψ and Δ contains Γ and has left dimensionality $[\Delta:\Gamma]_L = 2$ then Δ is Galois over Γ. On the other hand, we shall construct a class of examples where $[\Delta:\Gamma]_L = 2 = [\Delta:\Gamma]_R$, Γ of characteristic $\neq 2$ and Δ is not Galois over Γ.

We prove first a general theorem on dimensionalities as follows.

THEOREM 1. *Let Δ be a division ring, Γ a division subring, Φ and Ψ the centers of Δ and Γ respectively.* (1) *If $[\Delta:\Gamma]_L < \infty$ and $[\Gamma:\Psi] < \infty$ then $[\Delta:\Phi] < \infty$.* (2) *If $[\Delta:\Phi] < \infty$ then $[\Gamma:\Psi] \leqq [\Delta:\Phi]$, the equality holding if and only if the division subring $\Phi(\Gamma)$ generated by Φ and Γ coincides with Δ.*

Proof. (1) Our assumptions here imply that $[\Delta:\Psi]_L < \infty$. The result will therefore follow from the fact, which we proceed to prove, that if a division ring Δ is of finite left dimensionality over a subfield Ψ then Δ is of finite dimensionality over its center. Let $\delta_1, \delta_2, \cdots, \delta_n$ be elements of Δ which are linearly independent over Φ. Then it is well known that the right multiplications $\delta_{1R}, \delta_{2R}, \cdots, \delta_{nR}$ are linearly independent over the division ring Δ_L of left multiplications. Hence δ_{iR} are linearly independent over Ψ_L the subfield of Δ_L determined by Ψ. On the other hand, the ring $\mathfrak{L}$ of linear transformations of the left vector space Δ over Ψ contains Ψ_L since Ψ is commutative. Moreover, $[\mathfrak{L}:\Psi_L] \leqq [\Delta:\Psi]_L{}^2$. Since the $\delta_{iR} \in \mathfrak{L}$ this implies that $n \leqq [\Delta:\Psi]_L{}^2$. Hence $[\Delta:\Phi] \leqq [\Delta:\Psi]_L{}^2$. (2) If $x_1, x_2, \cdots, x_r$ are

* Received January 4, 1955.

[1] This research was supported in part by a grant from the National Science Foundation.

[2] [4]. Cf. also [1].

elements of a ring then we define $[x_1x_2\cdots x_r] = \sum_P \pm x_{i_1}x_{i_2}\cdots x_{i_r}$ where the summation is over all the permutations $(i_1, i_2, \cdots, i_r)$ of $(1, 2, \cdots, r)$ and the sign is $+$ or $-$ according as the permutation is even or odd. It has been shown by Amitsur and Levitzki ([2]) that if Φ_n is the ring of $n \times n$ matrices over a field Φ then $[x_1x_2\cdots x_{2n}] = 0$ for all $x_i \in \Phi_n$ but there exist $x_1, x_2, \cdots, x_{2n+1}$ in Φ_n such that $[x_1x_2\cdots x_{2n+1}] \neq 0$. This implies by the usual base field extension argument that if Δ is a division ring which is n^2 dimensional[3] over its center then $[x_1x_2\cdots x_{2n}] \equiv 0$ in Δ but $[x_1x_2\cdots x_{2n+1}] \not\equiv 0$ in Δ. Also it is a known result of Kaplansky's ([7]) that if $[\Delta:\Phi] = \infty$ then Δ satisfies no polynomial identity with coefficients in Φ. It is clear from these results that $[\Delta:\Phi] < \infty$ implies $[\Gamma:\Psi] \leqq [\Delta:\Phi]$. Now consider $\Phi(\Gamma)$. This is a subspace of Δ over Φ; hence it is finite dimensional. Let $\gamma_1, \gamma_2, \cdots, \gamma_r$ be a maximal set of elements of Γ which are linearly independent over Φ and let V be the Φ-space spanned by these. Evidently $\Gamma \subseteq V$. Hence V is a subring of Δ. Since V is finite dimensional over Φ it is a division subring. Thus $V = \Phi(\Gamma)$. Suppose $[\Gamma:\Psi] = m^2$, then $[\gamma_{i_1}\gamma_{i_2}\cdots\gamma_{i_{2m}}] = 0$ for all choices of $i_j = 1, 2, \cdots, r$. Hence $[x_1x_2\cdots x_{2m}] \equiv 0$ in $\Phi(\Gamma) = V$ so that if $\mathfrak{P}$ is the center of $\Phi(\Gamma)$, then $[\Phi(\Gamma):\mathfrak{P}] \leqq m^2$. On the other hand, if $[x_1x_2\cdots x_{2k}] \equiv 0$ in $\Phi(\Gamma)$ then the same holds in Γ. It follows that $[\Gamma:\Psi] \leqq [\Phi(\Gamma):\mathfrak{P}]$. Hence $[\Gamma:\Psi] = [\Phi(\Gamma):\mathfrak{P}] = m^2$. Now if $[\Gamma:\Psi] = [\Delta:\Phi] = n^2$ then $[\Phi(\Gamma):\mathfrak{P}] = n^2$ and, since $\mathfrak{P} \supseteq \Phi$, $[\Phi(\Gamma):\Phi] = n^2$. Thus $\Phi(\Gamma) = \Delta$. The converse is clear by the same argument.

THEOREM 2. *Let Γ be finite dimensional over its center Ψ and let Δ be a division ring containing Γ and such that $[\Delta:\Gamma]_L = 2$. Then if the characteristic is $\neq 2$, Δ is Galois over Γ.*

Proof. Theorem 1 shows that $[\Delta:\Phi] < \infty$ for Φ the center of Δ. We distinguish two cases; I. $\Gamma \supset \Phi$. Let $\mathfrak{C}(\Gamma)$ denote the centralizer of Γ in Δ. Then it is well known that $\mathfrak{C}(\mathfrak{C}(\Gamma)) = \Gamma$ so that Γ is the set of invariants of the inner automorphisms determined by the non-zero elements of $\mathfrak{C}(\Gamma)$. II. $\Gamma \not\supset \Phi$. Let $t \in \Phi, \not\in \Gamma$. Then $\Delta = \Gamma(t)$ and $t^2 = \gamma_1 t + \gamma_2$, $\gamma_i \in \Gamma$. Since t and t^2 commute with every $\gamma \in \Gamma$ this gives $(\gamma\gamma_1)t + \gamma\gamma_2 = (\gamma_1\gamma)t + \gamma_2\gamma$. Hence $\gamma\gamma_i = \gamma_i\gamma$ and so that γ_i are in the center Ψ of Γ. Since $\Delta = \Gamma(t)$ where $t \in \Phi$ it is clear that $\Psi = \Gamma \cap \Phi$. Hence the $\gamma_i \in \Phi$. We may replace t by $u = t - \frac{1}{2}\gamma_1$ and obtain $u^2 = \delta \in \Phi$. For $\alpha, \beta \in \Gamma$, the mapping $\alpha + \beta u \to \alpha - \beta u$ is an automorphism in Δ whose set of invariants is Γ.[4]

[3] It is well known that if Δ is finite over its center then its dimensionality over the center is a square.

[4] I am indebted to the referee for the following remark: In part II of the above

In the remainder of this note we shall construct some examples of two dimensional non-Galois extensions. These will be given as certain Clifford algebras of infinite dimensionality. We shall therefore begin by indicating that the well-known results on finite dimensional Clifford algebras can be carried over to the infinite case.

Let M be a vector space over a field Φ and let $Q(x)$ be a quadratic form on M. We denote the associated scalar product $Q(x+y)-Q(x)-Q(y)$ by (x,y). This is symmetric and if the characteristic is two then (x,y) is alternate: $(x,x)=0$. If N is a subspace we define $N^{\perp}=\{y \mid (x,y)=0, x \in N\}$. N is isotropic if $N \cap N^{\perp} \neq \{0\}$, totally isotropic if $N \subseteq N^{\perp}$. The scalar product (and the quadratic form) is non-degenerate if $M^{\perp} \neq \{0\}$, totally regular if there exists no isotropic $((x,x)=0)$ $x \neq 0$.

Let $\mathfrak{F}$ be the free algebra $\mathfrak{F}=\Phi 1 \oplus M \oplus (M \otimes M) \oplus (M \otimes M \otimes M) \oplus \cdots$ based on the space M and let $\mathfrak{B}$ be the ideal in F generated by $x \otimes x - Q(x)1$. Then $\Delta=\mathfrak{F}/\mathfrak{B}$ is called the *Clifford algebra* of M relative to Q.

It is easy to see that the natural homomorphism of M into Δ is an isomorphism ([3], p. 39). One may therefore consider M as a subspace of Δ. If N is a subspace of M, then the subalgebra of Δ generated by 1 and N is isomorphic, and so may be identified with the Clifford algebra $\Delta(N,Q)$ of N relative to the contraction of Q.[5]

From now on we assume that (x,y) is non-degenerate. Then it is well known that if M is even (finite) dimensional then Δ is central simple and if M is odd dimensional then Δ is a Kronecker product of a central simple algebra and a two dimensional semi-simple algebra. The structure of Δ can be described more precisely by using the following

LEMMA. *Let F be a non-isotropic subspace of $2\mu < \infty$ dimensions. Then the Clifford algebra $\Delta(M,Q)$ of M relative to Q is a Kronecker product $\Delta(F,Q) \otimes \Delta(F^{\perp}, (-1)^{\mu(2\mu-1)}\delta Q)$ of the Clifford algebra of F and Q and that of $F^{\perp}$ and $(-1)^{\mu(2\mu-1)}\delta Q$ where δ is the discriminant of (x,y) in F.*

Proof. Char. $\neq 2$. We choose an orthogonal basis $(u_1, u_2, \cdots, u_{2\mu})$ for F and set $(u_i, u_i)=\delta_i \neq 1$. Set $c=2^{2\mu}u_1u_2\cdots u_{2\mu}$. Since $u_iu_j=-u_ju_i$, for $i \neq j$, $u_i^2=\frac{1}{2}\delta_i 1$, $c^2=(-1)^{\mu(2\mu-1)}\delta$ where $\delta=\Pi\delta_i$ is the discriminant of (x,y). It is known that for finite dimensional non-isotropic subspaces

---

proof, no use is made of dimensionality relations. Hence the argument shows that if $[\Delta:\Gamma]_L=2$ for arbitrary Γ, and $\Gamma \supsetneq \Phi$, then Δ is the Kronecker product over Ψ of Γ and a quadratic extension of Ψ.

[5] It suffices to prove this for finite dimensional N. The arguments given in [3] suffice in this case. If N is even dimensional and non-isotropic then the lemma given below can also be used. An easy reduction can be made to this special case.

$F, M = F \oplus F^{\perp}$. If $x \in F^{\perp}$, $xc = cx$ and $(cx)^2 = Q(x)(-1)^{\mu(2\mu-1)}\delta$. It follows easily that the subalgebra generated by the elements cx is the Clifford algebra $\Delta(F^{\perp}, (-1)^{\mu(2\mu-1)}\delta Q)$ and

$$\Delta(M, Q) = \Delta(F, Q) \otimes \Delta(F^{\perp}, (-1)^{\mu(2\mu-1)}\delta Q).$$

Char. $= 2$. Here we can choose a symplectic basis for F:

$$(u_1, v_1, u_2, v_2, \cdots, u_\mu, v_\mu)$$

with $(u_i, v_i) = 1 = (v_i, u_i)$ and all other products 0. The discriminant of (x, y) relative to this basis is 1. If $x \in F$, $y \in F^{\perp}$ then $xy = yx$. It follows that $\Delta(M, Q) = \Delta(F, Q) \otimes \Delta(F^{\perp}, Q)$.

This lemma shows that if M is of even dimensionality then Δ is a Kronecker product of generalized quaternion algebras and if M is odd dimensional then Δ is a Kronecker product of generalized quaternion algebras and a two dimensional semi-simple algebra. We now prove

THEOREM 3. *Let M be an infinite dimensional vector space with a non-degenerate quadratic form Q. Then the Clifford algebra $\Delta(M, Q)$ is central simple. Moreover, if $\dim M = \aleph_0$ then $\Delta(M, Q)$ is a Kronecker product of a countable number of generalized quaternion algebras and any such product can be obtained from a suitable Clifford algebra.*

Proof. The first statement will follow by showing that any finite subset S of $\Delta = \Delta(M, Q)$ is contained in a finite dimensional central simple subalgebra containing 1. By using a basis one sees that S is contained in the subalgebra generated by 1 and a finite dimensional subspace F. Since any finite dimensional subspace can be imbedded in a non-isotropic one, we may assume F non-isotropic. Also it is easy to see (using $M = F \oplus F^{\perp}$) that we may assume $\dim F = 2\mu$. Then the subalgebra $\Delta(F, Q)$ is central simple. Now suppose $\dim M = \aleph_0$. If $\text{char} \neq 2$ we denote the generalized quaternion algebra with basis $(1, i, j, ij)$ such that $i^2 = \alpha 1$, $j^2 = \beta 1$, $ij = -ji$ by (α, β) and if $\text{char.} = 2$ we denote the generalized quaternion algebra with basis $(1, i, j, ij)$ such that $i^2 = \alpha 1$, $j^2 = \beta 1$, $ij + ji = 1$ by $[\alpha, \beta]$. If $\text{char.} \neq 2$ we choose an orthogonal basis $(u_1, v_1, u_2, v_2, \cdots)$ with $Q(u_i) = \alpha_i$, $Q(v_i) = \beta_i$ ([8], p. 3). Then using $(\alpha\rho^2, \beta\rho^2) = (\alpha, \beta)$ for all $\rho \neq 0$ and the lemma, we obtain

$$\Delta = (\alpha_1, \beta_1) \otimes (-\alpha_1\beta_1\alpha_2, -\alpha_1\beta_1\beta_2) \otimes (-\alpha_2\beta_2\alpha_3, -\alpha_2\beta_2\beta_3)$$
$$\otimes \cdots \otimes (-\alpha_\nu\beta_\nu\alpha_{\nu+1}, -\alpha_\nu\beta_\nu\beta_{\nu+1}) \otimes \cdots.$$

If char. $= 2$ we choose a symplectic basis $(u_1, v_1, u_2, v_2, \cdots)$ with $(u_i, v_i) = 1 = (v_i, u_i)$ ([8], p. 4). If $Q(u_i) = \alpha_i$, $Q(v_i) = \beta_i$ then the above lemma gives the formula

$$\Delta = [\alpha_1, \beta_1] \otimes [\alpha_2, \beta_2] \otimes [\alpha_3, \beta_3] \otimes \cdots .$$

The last statement of the theorem is clear from the above formulas.

It has been shown by Koethe ([9]) that there exist infinite Kronecker products of quaternion algebras which are division algebras. We shall sketch an alternative proof. Let Γ be a given division ring with center Ψ. Then the polynomial domain $\Gamma[\lambda]$ is a principal ideal domain and so it can be imbedded in a quotient field $\Gamma(\lambda)$. The center of $\Gamma(\lambda)$ is $\Psi(\lambda)$. If char. $\neq 2$, we let S be the automorphism in $\Gamma(\lambda)$ which is the identitly on Γ and sends λ into $-\lambda$ and we form the semi-linear polynomial domain $\Gamma(\lambda)[t, S]$ of polynomials in t with coefficients in $\Gamma(\lambda)$ such that $ta = (aS)t$, $a \in \Gamma(\lambda)$ ([5], p. 29). This is a principal ideal domain and can be imbedded in a quotient field Δ. The center Φ of Δ is $\Psi(\lambda^2, t^2)$ and $\Delta = \Gamma(\lambda^2, t^2) \otimes_\Phi (\lambda^2, t^2)$ where $\Gamma(\lambda^2, t^2)$ is the division subring generated by Γ, λ^2, t^2. We can begin our construction with a field $\Gamma = \Phi_0$ and repeat this an infinite number of times to obtain a division algebra with center $\Phi(\lambda_1{}^2, t_1{}^2, \lambda_2{}^2, t_2{}^2, \cdots)$ which has the form $(\lambda_1{}^2, t_1{}^2) \otimes (\lambda_2{}^2, t_2{}^2) \otimes \cdots$ over this center. If char. $= 2$ we modify the construction by replacing the automorphism S by the derivation D in $\Gamma(\lambda)$ such that $\Gamma D = \{0\}$ and $\lambda D = 1$. Then we consider the differential polynomial domain $\Gamma(\lambda)[t, D]$ with $ta = at + aD$. In the end we obtain the center $\Phi_0(\lambda_1{}^2, t_1{}^2, \lambda_2{}^2, t_2{}^2, \cdots)$ and the division algebra

$$[\lambda_1{}^2, t_1{}^2] \otimes [\lambda_2{}^2, t_2{}^2] \otimes \cdots$$

over this center.

We now suppose that $\Delta = \Delta(M, Q)$ is a Clifford algebra of a space M relative to a quadratic form Q and that Δ is a division ring. Let H be a hyperplane in M, so that $M = H \oplus \Phi u$ where $u \in M$ and Φ is the base field. Let $\Gamma = \Delta(H, Q)$ be the subalgebra generated by 1 and H. Since the elements of Δ are algebraic over Φ, Γ is a division ring. We have the relation $ux = -xu + (x, u)1$ for $x \in H$. Hence if $a \in \Gamma$ then we have a relation of the form $ua = (aI)u + aD$ where aI and aD are elements in Γ. Since $u \notin \Gamma$ the elements aI and aD are uniquely determined by a. One verifies that I is an isomorphism of Γ into itself and D is an I-derivation: $(ab)D = (aI)(bD) + (aD)b$. Since the image under I contains H it is clear that I is an automorphism. The relations $ua = (aI)u + (aD)$, $u^2 = Q(u)1$ show that

$(1, u)$ is both a left basis and a right basis for Δ over Γ. Hence $[\Delta:\Gamma]_L = 2 = [\Delta:\Gamma]_R$. We now prove

THEOREM 4. *Let $\Delta = \Delta(M, Q)$ be a Clifford division algebra determined by a vector space M relative to a quadratic form Q and let $\Gamma = \Delta(H, Q)$ be the subalgebra generated by 1 and a hyperplane H. Assume char. $\neq 2$. Then Δ is Galois over Γ if and ony if $H^\perp \neq \{0\}$.*

Proof. Since Δ is a division ring, M contains no isotropic vectors. Hence $H \cap H^\perp \neq \{0\}$. If $H^\perp \neq \{0\}$ we choose u in this space. Then we have $ua = (aI)u$ and we have an automorphism mapping every $a \in \Gamma$ into itself and mapping u into $-u$. The set of invariants relatively to this automorphism is Γ. Hence Γ is Galois in Δ. Conversely, assume Δ is Galois over Γ. Then it is known that $\Delta = \Gamma(t)$ where t is an element such that the inner automorphism determined by t maps Γ into itself. Write $t = cu + d, c, d \in \Gamma$, $c \neq 0$. We may replace t by $v = c^{-1}t = u + e$, $e = c^{-1}d$. If $a \in \Gamma$ the condition $va = a_1 v$, $a_1 \in \Gamma$ gives $a_1 = aI$ and $aD = (aI)e - ea$. In particular, if $x \in H$, then $(x, u)1 = -(xe + ex)$. If M is finite dimensional then it is clear that $H^\perp \neq \{0\}$. Hence we may assume M infinite dimensional. Then we can find an even dimensional subspace F in H such that $e \in \Delta(F, Q)$ the subalgebra generated by 1 and F. Since Q is non-degenerate in F we can find a $u' \in F$ such that $(x, u') = (x, u)$ for all $x \in F$. Hence if $v' = u' + e$ then $xv' + v'x = 0, x \in F$. If $(u_1, v_1, \cdots, u_\mu, v_\mu)$ is an orthogonal basis for F, the element $u_1 v_1 \cdots u_\mu v_\mu$ has an inverse and anti-commutes with every $x \in F$. Since $\Delta(F, Q)$ is central this implies that $v' = \rho u_1 v_1 \cdots u_\mu v_\mu$. We now imbed F in a space G in H of $(2\mu + 2)$-dimensions with orthogonal basis $(u_1, v_1, \cdots, u_{\mu+1}, v_{\mu+1})$. Since $e = \rho u_1 v_1 \cdots u_\mu v_\mu - u'$, the relation $(u_{\mu+1}, u)1 = -(u_{\mu+1}e + eu_{\mu+1})$ gives $(u_{\mu+1}, u)1 = -2\rho u_1 v_1 \cdots u_\mu v_\mu u_{\mu+1}$. Hence $\rho = 0$ and $e = -u' \in H$. Then $(x, u) = (x, u')$ for all $x \in H$ and $u - u' \neq 0$ is in $H^\perp$, Thus $H^\perp \neq \{0\}$.

If M is an $\aleph_0$ dimensional space over a field of characteristic $\neq 2$ and Q is a quadratic form whose associated scalar product is non-degenerate, then we can always find hyperplanes H in M such that $H^\perp = \{0\}$. This is easily seen by using an orthogonal basis. This remark and Theorem 4 show that there exist two dimensional non-Galois extensions of division rings of Char. $\neq 2$.

YALE UNIVERSITY.

REFERENCES.

[1] A. S. Amitsur, "Non-commutative cyclic fields," *Duke Mathematical Journal*, vol. 21 (1954), pp. 87-106.

[2] ——— and J. Levitzki, "Minimal identities for algebras," *Proceedings of the American Mathematical Society*, vol. 1 (1950), pp. 449-463.

[3] C. C. Chevalley, *The Algebraic Theory of Spinors*, New York, 1954.

[4] J. Dieudonné, "Les extensions quadratiques des corps non-commutatifs et leurs applications," *Acta Mathematica*, vol. 87 (1952), pp. 175-242.

[5] N. Jacobson, *The Theory of Rings*, New York, 1943.

[6] ———, "Structure of alternative and Jordan bimodules," *Osaka Mathematics Journal*, vol. 6 (1954), pp. 1-71.

[7] I. Kaplansky, "Rings with a polynomial identity," *Bulletin of the American Mathematical Society*, vol. 54 (1948), pp. 575-580.

[8] ———, "Forms in infinite-dimensional spaces," *Academie Brasiliera de Ciencias*, vol. 22 (1950), pp. 1-16.

[9] G. Koethe, "Schiefkörper unendlichen Ranges über dem Zentrum," *Mathematische Annalen*, vol. 105 (1931), pp. 15-39.

ON THE ORTHOGONALIZATION OF OPERATOR REPRESENTATIONS.*

By RICHARD V. KADISON.

---

1. Introduction. The main problem with which we shall be concerned is that of finding conditions under which a group representation is similar to a unitary representation and conditions for a representation of a self-adjoint algebra of operators on a Hilbert space to be similar to an adjoint preserving representation (* representation). These situations are slightly different aspects of the representation orthogonalization process with very close interconnections. With regard to the algebra situation one can phrase the main question in the following way. *Is an algebra of operators on a Hilbert space which is the isomorphic image of a C*-algebra (uniformly closed self-adjoint algebra of operators) similar to a C*-algebra in such a way that the composition of the isomorphism and the similarity is an adjoint preserving representation of the C*-algebra?* The question for group representations takes the following form. *Is every bounded representation of a group by operators on a Hilbert space similar to a unitary representation, where, by "bounded representation" we mean that there exists a constant such that each representing operator is, in norm, less than this constant?* In this form, the group question has been raised before, notably in [1], [2], [5]. The question of when a group admits a mean (or Banach Limit) is the primary consideration of these papers and then, employing the technique of [4], it is shown that for such groups all bounded representations (continuous in the strong topology) are similar to unitary representations (this is done in [4] for the infinite cyclic group and the reals). We outline this technique. A (left, right) mean on a group G is a positive linear functional on the linear space $B(G)$ of bounded continuous functions on G which takes the value 1 at the constant function 1 and which is invariant under (left, right) translations on the group. If G admits a right mean m and $g \to A_g$ is a strongly continuous representation of the group by operators on a Hilbert space, then, for each x, y in the Hilbert space $g \to (A_g x, A_g y)$ is a bounded continuous function on G and $\langle x, y \rangle = m((A_g x, A_g y))$ is an inner product on the Hilbert

---

* Received February 17, 1954; revised February 1, 1955.

space giving rise to a norm equivalent to the original norm and under which the operators A_g are unitary. It is then standard to find the similarity of the original Hilbert space which takes each A_g into a unitary operator. Continuity considerations do not enter into the question of whether all bounded representations of all groups are similar to unitary representations since it is obviously sufficient to settle this for discrete groups. With regard to the technique of means, it is well-known that many groups admit neither a left nor right mean (in the sense noted above, e. g., the free group on two generators; see [1], [2]) so that this method cannot, in itself, give the full answer.

Our concern is not with conditions on the group which imply that bounded representations are similar to unitary representations but rather with restrictions upon the representations which insure that they are similar to unitary representations. We feel that this approach gives hope of settling the full question one way or the other.

The truth of the operator algebra proposition is trivially implied by the truth of the group statement (see the proof of Theorem 7). On the other hand, a bounded representation of a group (discrete) can be extended to a representation of its L_1 algebra (as a self-adjoint algebra of operators acting by convolution on L_2). This algebra of operators need not be closed in the uniform operator topology and the representation need not be extendable to the uniform closure of this algebra; so that it would appear that the truth of the algebra result would imply the group conjecture only for those bounded representations which are extendable to the uniform closure of the L_1 algebra. (The similarity which transforms the representation of the L_1 algebra into a * representation will transform the group representation into a unitary representation). However, it is possible to renorm the L_1 algebra in such a way that the completion of the resulting * algebra is a C^*-algebra to which each bounded group representation is extendable, by assigning to each element of the L_1 algebra the supremum of the norms of its images in each * representation. It follows from the existence of a Banach algebra norm on L_1 in which the * map is isometric (viz., the L_1 norm) that this supremum is not greater than the L_1 norm (and certainly finite). Our extended group representation, being a bounded algebra representation relative to the L_1 norm on the L_1 algebra of the group, is a continuous representation of the L_1 algebra in the C^* norm just constructed. Although the representation extended to this C^*-algebra may not be an isomorphism, the kernel is a closed two-sided ideal so that the factor algebra is a C^*-algebra [8], and the induced representation on this factor C^*-algebra is an isomorphism. Thus we have the

complete equivalence of the group and C^*-algebra questions. We are indebted to I. Kaplansky for bringing to our attention the known renorming device used above. It is possible that a more incisive operator algebra result would apply directly to the L_1 algebra (acting by convolution on L_2). In [6], Mackey proves the algebra result in the commutative case by direct methods (this result follows at once, as in the proof of Theorem 7, from the fact that commutative groups have means, in the sense defined above; see [5]).

The origin of the group question can be found in the classical statement which says that each representation of a finite group by (complex, real) matrices is equivalent to a representation by (unitary, orthogonal) matrices and its extension to continuous representations of compact groups [7]. The technique used in these proofs, invariant integration over the group, is almost identical with the technique of means. Using this theorem for compact groups the operator algebra result follows for finite-dimensional operator algebras (applied to the (compact) group of unitary operators in the algebra). Perhaps a more natural way of concluding the algebra result in the finite-dimensional case is thru the semi-simplicity of the image algebra. In this case the various concepts of semi-simplicity coincide so that the semi-simplicity of the original C^*-algebra, interpreted algebraically, is inherited by the image, and this, interpreted spatially, shows that this image is similar to a C^*-algebra. In the infinite-dimensional case it is not at all difficult to construct an algebra of operators which is semi-simple in all the conventional senses but not similar to a C^*-algebra. The following topological difficulty can occur: while each invariant subspace may have a complementary invariant subspace, the greatest of the angles between the given space and all possible invariant complements may tend to 0 for some sequence of invariant subspaces, thus ruling out what we may call the "topological semi-simplicity" of the algebra. For a C^*-algebra and a unitary group, the orthogonal complement of an invariant subspace is invariant. Our similarity problem for the given family of operators (group or algebra) amounts to an orthogonalization process.

In Section 2, we begin by defining concepts of local semi-simplicity and bounded local semi-simplicity of group representations. Theorem 1 states that bounded local semi-simplicity of a group representation is necessary and sufficient for the representation to be similar to a unitary representation. Several different forms of a conjecture concerning the group question are discussed, with the aid of Theorem 1. To study the operator algebra question, we develop a device for measuring the deviation of a set of vectors from being an orthonormal set. After stating a condition for a representation of a C^*-

algebra to be similar to a * representation in terms of the group condition (Theorem 1), we employ this device to give a more delicate criterion for topological semi-simplicity of an algebra of operators. In the concluding section, we discuss some extensions of the results stated, examples, and a class of natural questions an affirmative answer to any of which would yield the fact that all bounded operators on a Hilbert space have non-trivial, closed, invariant subspaces.

2. Conditions for topological semi-simplicity. The following definition contains a description of local behavior of a group representation, which is necessary and sufficient for the group representation to be similar to a unitary representation. The statement and proof of this fact are contained in Theorem 1.

DEFINITION 1. *A representation $g \to A_g$ of the group G by bounded operators A_g on the Banach space $\mathfrak{B}$ is said to be "locally semi-simple" when, for each finite set $x_1, \cdots, x_n$ of vectors in $\mathfrak{B}$ and $g_1, \cdots, g_n$ of elements in G, one can find a linear transformation S defined on the finite-dimensional vector space $\mathfrak{V}$ generated by $x_1, \cdots, x_n, A_{g_1}x_1, \cdots, A_{g_n}x_n$ such that $\| Sx_i \| = \| SA_{g_i}x_i \|$; $i = 1, \cdots, n$. If there exists a constant M such that S can always be chosen satisfying*

$$1/M \leqq \inf \{ \| Sx \| : x \in \mathfrak{V}, \| x \| = 1 \};$$
$$M \geqq \sup \{ \| Sx \| : x \in \mathfrak{V}, \| x \| = 1 \},$$

we say that the representation is "boundedly locally semi-simple."

THEOREM 1. *A representation $g \to A_g$ of the group G by bounded operators A_g on a Hilbert space $\mathfrak{H}$ is boundedly locally semi-simple if and only if it is similar to a unitary representation.*

Proof. The necessity of the condition is quite easy. Indeed, suppose that S is a bounded invertible operator on $\mathfrak{H}$ such that SA_gS^{-1} is unitary for each g in G. Let $x_1, \cdots, x_n$ in $\mathfrak{H}$ and $g_1, \cdots, g_n$ in G be given. Since SA_gS^{-1} is unitary we have

$$\| SA_{g_i}x_i \| = \| SA_{g_i}S^{-1}Sx_i \| = \| Sx_i \|; \qquad i = 1, \cdots, n,$$

which establishes the bounded local semi-simplicity of the given representation.

Suppose now that the given group representation is known to be boundedly locally semi-simple and that M is a bounding constant. We establish, in the succeeding lemmas, the existence of an invertible operator

P with $\| P \|$, $\| P^{-1} \|$ not exceeding M and such that $P^{-1}A_gP$ is unitary for each g in G.

LEMMA 2. *If $\mathcal{V}$ is a finite-dimensional subspace of $\mathcal{H}$ there exists a Hilbert space norm $\| \ \|'$ on $\mathcal{V}$ such that $\| A_g x \|' = \| A_{g'} x \|'$ whenever $A_g x$ and $A_{g'} x$ are in $\mathcal{V}$ and such that $1/M \| y \| \leqq \| y \|' \leqq M \| y \|$ for each vector y in $\mathcal{V}$.*

Proof. We endow the conjugate tensor product $\mathcal{V} \otimes \mathcal{V}$ (i.e., the tensor product which is conjugate linear in the second variable, $x \otimes \alpha y = \bar{\alpha}(x \otimes y)$) with the natural inner product derived from the inner product of $\mathcal{H}$, i.e., we define $\langle x \otimes y, z \otimes w \rangle = (x, z)(w, y)$ and extend the domain of definition of this inner product to all of $\mathcal{V} \otimes \mathcal{V}$ by bilinearity. It is well-known that this process gives rise to an inner product (independent) of the representation of the elements involved as a sum of elements of the form $x \otimes y$—(see [3], for example).

Let $\mathcal{V}\otimes$ be the subspace of $\mathcal{V} \otimes \mathcal{V}$ generated by tensors of the form $x \otimes x$, and let $\mathcal{E}\otimes$ be the subspace of $\mathcal{V}\otimes$ generated by vectors of the form $A_g y \otimes A_g y - y \otimes y$, where y and $A_g y$ are in $\mathcal{V}$. Choose a basis

$$A_{g_1} y_1 \otimes A_{g_1} y_1 - y_1 \otimes y_1, \cdots, A_{g_m} y_m \otimes A_{g_m} y_m - y_m \otimes y_m$$

for $\mathcal{E}\otimes$. By the bounded local semi-simplicity of the representation $g \to A_g$, we can find a linear transformation S such that $\| SA_{g_i} y_i \| = \| Sy_i \|$; $i = 1, \cdots, m$ and

$$1/M \leqq \inf \{ \| Sy \| : y \text{ in } \mathcal{V}', \| y \| = 1 \};$$
$$M \geqq \sup \{ \| Sy \| : y \text{ in } \mathcal{V}', \| y \| = 1 \},$$

where $\mathcal{V}'$ is the subspace of $\mathcal{V}$ generated by $y_1, \cdots, y_m, A_{g_1} y_1, \cdots, A_{g_m} y_m$. By defining S to be a suitable scalar (between $1/M$ and M) on $\mathcal{V} \ominus \mathcal{V}'$, we obtain a linear transformation, which we denote again by S, defined on all of $\mathcal{V}$ and satisfying the same conditions as above with $\mathcal{V}$ replacing $\mathcal{V}'$ (no difficulties can arise if we choose S so that $S(\mathcal{V}') = \mathcal{V}'$ by composing the original S with a unitary transformation).

Let $\tilde{x} = \sum_{j=1}^{n} S^* x_j \otimes S^* x_j$, where $x_1, \cdots, x_n$ is an orthonormal basis for $S(\mathcal{V})$. Observe that

$$\langle \tilde{x}, A_{g_i} y_i \otimes A_{g_i} y_i - y_i \otimes y_i \rangle = \sum_{j=1}^{n} (S^* x_j, A_{g_i} y_i)(A_{g_i} y_i, S^* x_j)$$
$$- \sum_{j=1}^{n} (S^* x_j, y_i)(y_i, S^* x_j) = \sum_{j=1}^{n} |(x_j, SA_{g_i} y_i)|^2 - \sum_{j=1}^{n} |(x_j, Sy_i)|^2$$
$$= \| SA_{g_i} y_i \|^2 - \| Sy_i \|^2 = 0,$$

as follows from the fact that $SA_{\varrho_i}y_i$, Sy_i are in $S(\mathcal{V})$, the Parseval equality, and the choice of S. Consequently $\tilde{x}$ is orthogonal to $\mathcal{E}\otimes$. We define a new inner product on $\mathcal{V}$ by means of $(x,y)' = \langle x\otimes y, \tilde{x}\rangle$ so that the new Hilbert norm on $\mathcal{V}$ satisfies

$$\| y \|' = \langle y\otimes y, \tilde{x}\rangle^{\frac{1}{2}} = [\sum_{j=1}^{n} (S^*x_j, y)\,(y, S^*x_j)\,]^{\frac{1}{2}}$$

$$= [\sum_{j=1}^{n} |\,(x_j, Sy)\,|^2]^{\frac{1}{2}} = \| Sy \|.$$

It follows at once from this last equality that $1/M \| y \| \leqq \| y \|' \leqq M \| y \|$. If now y and $A_\varrho y$ are in $\mathcal{V}$ then $A_\varrho y\otimes A_\varrho y - y\otimes y$ is in $\mathcal{E}\otimes$ so that

$$0 = (A_\varrho y\otimes A_\varrho y - y\otimes y, \tilde{x}) = (A_\varrho y\otimes A_\varrho y, \tilde{x}) - (y\otimes y, \tilde{x})$$

$$= (\| A_\varrho y \|')^2 - (\| y \|')^2$$

or $\| y \|' = \| A_\varrho y \|'$. If $A_\varrho x$ and $A_{\varrho'}x = A_{\varrho'}A_{\varrho-1}(A_\varrho x)$ are in $\mathcal{V}$, then $\| A_\varrho x \|' = \| A_{\varrho'}x \|'$, which completes the proof of this lemma.

The following lemma allows us to pass from our finite-dimensional information to information about the full space on which the A_ϱ operate.

LEMMA 3. *If $\mathcal{B}$ is a Banach space and ρ is a partition function on $\mathcal{B}$ such that on each finite-dimensional subspace $\mathcal{B}_1$ of $\mathcal{B}$ one can introduce a norm $\| \|'$ in which $\mathcal{B}_1$ is a Hilbert space, each partition class intersected with $\mathcal{B}_1$ lies on the shell of some sphere center at 0 in the norm $\| \|'$, and there exists a constant M (depending upon ρ) such that*

$$1/M \| x \| \leqq \| x \|' \leqq M \| x \|$$

for each x in $\mathcal{B}_1$ (where $\| \|$ is the norm on $\mathcal{B}$); then the underlying vector space of $\mathcal{B}$ admits a norm, equivalent to the original norm, in which it is a Hilbert space and such that the partition classes of ρ each lie on the shell of some sphere center at 0 relative to the new norm.

Proof. We form a product of intervals with $\mathcal{B}$ as the indexing family. To each point x in $\mathcal{B}$, we make correspond the closed interval $[\| x \|/M, M \| x \|]$ (thus to 0 in $\mathcal{B}$ we make correspond the number 0). Denote by X the Cartesian product

$$\prod_{x\in\mathcal{B}} I_x = \prod_{x\in\mathcal{B}} [\| x \|/M, M \| x \|].$$

We consider X in its standard product topology, in which it is compact, where each I_x is given its usual metric topology. Let $\mathcal{B}_1$ be a finite-dimensional

subspace of $\mathfrak{B}$, and let $X(\mathfrak{B}_1)$ be the set of points of X which as functions restricted to $\mathfrak{B}_1$ give rise to a Hilbert space norm on $\mathfrak{B}_1$ which is constant on the partition classes of ρ intersected with $\mathfrak{B}_1$. We shall show presently that $X(\mathfrak{B}_1)$ is a closed subset of X. Assume, for the moment, that we have proved this fact. The sets $X(\mathfrak{B}_1)$ have the finite intersection property ($\mathfrak{B}_1$ ranging over the finite-dimensional subspaces of $\mathfrak{B}$). Indeed, let $\mathfrak{B}_1, \cdots, \mathfrak{B}_n$ be a (finite) set of finite-dimensional subspaces of $\mathfrak{B}$ and let $\mathfrak{B}_0$ be the (finite-dimensional) subspace they generate. By assumption, we can find a Hilbert space norm $\| \ \|_0$ on $\mathfrak{B}_0$ which is constant on the partition classes of ρ intersected with $\mathfrak{B}_0$, and which satisfies the inequality

$$1/M \| x \| \leqq \| x \|_0 \leqq M \| x \|$$

for each x in $\mathfrak{B}_0$. The function which assigns to each x not in $\mathfrak{B}_0$ the value $M \| x \|$ and to each x in $\mathfrak{B}_0$ the value $\| x \|_0$ lies in $X(\mathfrak{B}_0)$ which is clearly contained in $\bigcap_{i=1}^{n} X(\mathfrak{B}_i)$. It now follows from the compactness of X (and our assumption that the sets $X(\mathfrak{B}_1)$ are closed in X) that the intersection of all the sets $X(\mathfrak{B}_1)$ is not empty. Let $\| \ \|'$ be a function on $\mathfrak{B}$ in this intersection. Then, on each finite-dimensional subspace of $\mathfrak{B}$, $\| \ \|'$ induces a Hilbert space norm. It is immediate that $\| \ \|'$ satisfies the norm axioms and the Parallelogram Law on $\mathfrak{B}$ as well as being constant on the partition classes of ρ, so that $\| \ \|'$ is our desired Hilbert space norm on $\mathfrak{B}$. Of course $1/M \| x \| \leqq \| x \|' \leqq M \| x \|$, since $\| \ \|'$ is in X. It remains to prove that the sets $X(\mathfrak{B}_1)$ are closed in X. We shall omit this proof, however, since it is a standard approximation argument of the type employed in the proof of the w^*-compactness of the unit sphere in the conjugate space of a normed linear space.

Proof of Theorem 1. As partition function ρ on $\mathfrak{H}$ we take the map which assigns to each vector x in $\mathfrak{H}$ the set of vectors $\{A_g x : g \text{ in } G\}$. Since the family of operators $\{A_g\}$ forms a group, this map defines a partition function on $\mathfrak{H}$. Lemma 2 establishes the hypothesis of Lemma 3 with this partition function and $\mathfrak{H}$ for $\mathfrak{B}$, so that we can conclude the existence of a norm $\| \ \|'$ on $\mathfrak{H}$ in which $\mathfrak{H}$ is a Hilbert space and such that $\| A_{g_1} x \|' = \| A_{g_2} x \|'$ for each x in $\mathfrak{H}$ and g_1, g_2 in G. In particular $\| x \|' = \| A_g x \|'$ so that each operator A_g is isometric with respect to the norm $\| \ \|'$. Moreover, $\| \ \|'$ can be so chosen that $\| x \|/M \leqq \| x \|' \leqq M \| x \|$ for each vector x in $\mathfrak{H}$.

Let $x_1, \cdots$ be an orthonormal basis for $\mathfrak{H}$ with respect to the norm $\| \ \|$

(and associated inner product (,)), and let $y_1, \cdots$ be an orthonormal basis for $\mathcal{H}$ with respect to the norm $\| \ \|'$ (and associated inner product (,)'). Define a linear transformation P of $\mathcal{H}$ into itself by $Px_i = y_i$; $i = 1, \cdots$. Then

$$(x, y) = (\sum_i (x, x_i)x_i, \sum_i (y, x_i)x_i) = \sum_i (x, x_i)(x_i, y)$$
$$= (\sum_i (x, x_i)y_i, \sum_i (y, x_i)y_i)' = (Px, Py)'.$$

Of course $(P^{-1}x, P^{-1}y) = (x, y)'$, substituting $P^{-1}x$ for x and $P^{-1}y$ for y throughout the above equality. We assert that $P^{-1}A_gP$ is a unitary operator on $\mathcal{H}$ with respect to the norm $\| \ \|$ for each g in G. Indeed,

$$(P^{-1}A_gPx, P^{-1}A_gPy) = (A_gPx, A_gPy)' = (Px, Py)' = (x, y).$$

We note in conclusion that $\| P \|$, $\| P^{-1} \|$ do not exceed M. In fact, if $x = \sum_i \alpha_i x_i$ with $1 = \| x \|^2 = \sum_i |\alpha_i|^2$ is given, then $\| Px \|' = \| \sum_i \alpha_i y_i \|' = 1$ and $\| Px \|/M \leqq \| Px \|' \leqq M \| Px \|$, so that $1/M \leqq \| Px \| \leqq M$.

There are several ways of formulating a conjecture concerning the classical question of whether or not each bounded representation of a group is similar to a unitary representation.

CONJECTURE A. *Every bounded representation of a group by operators on a Hilbert space is similar to a unitary representation.*

CONJECTURE B. *There exists a function f from the positive reals to the positive reals with the property that for each bounded representation $g \to A_g$ with bound M, of a group G by operators on a Hilbert space one can find an invertible operator P such that $P^{-1}A_gP$ is unitary for each g in G and such that $\| P \|$, $\| P^{-1} \|$ do not exceed $f(M)$.*

CONJECTURE C. *Same as* B *with f as the identity transform.*

Each of the above conjectures is clearly stronger than the preceding one. We shall show that B is actually equivalent to A in the next lemma.

LEMMA 4. *Conjecture* A *is equivalent to Conjecture* B.

Proof. Clearly B implies A. Suppose now that A is true. If B is false there exists a sequence of groups $G_1, G_2, \cdots$ and a sequence of representations $g^{(1)} \to A_{g^{(1)}}$, $g^{(2)} \to A_{g^{(2)}}, \cdots$ of these groups, respectively, each with bound M and such that if $N_i = \inf\{\max(\| P_i \|, \| P_i^{-1} \|) : P_i^{-1}A_{g^{(i)}}P_i$ unitary for each $g^{(i)}$ in $G_i\}$ then $\lim_i N_i = \infty$. Let $G = G_1 \otimes G_2 \otimes \cdots$ be the weak direct

sum of the groups $G_1, G_2, \cdots$, and let $g \to A_g$ be the direct sum of the representations $g^{(1)} \to A_{g^{(1)}}, \cdots$. The representation $g \to A_g$ of G has bound M. Assuming A, we can find an operator P such that $P^{-1}A_gP$ is unitary for each g in G. Restricted to each direct summand, this similarity induces similarities of all the representations $g^{(i)} \to A_{g^{(i)}}$, each similarity with bound not greater than $\max(\| P \|, \| P^{-1} \|)$—a contradiction. Hence A implies B.

THEOREM 5. *If* B *is true for the free groups on finitely many generators then* B *is true for all groups.*

Proof. Let $g \to A_g$ be a representation of G with bound M. We shall show that this representation is boundedly locally semi-simple with bounding constant $f(M)$. In fact, let $x_1, \cdots, x_n$ in $\mathfrak{H}$ and $g_1, \cdots, g_n$ in G be given. The group G_n generated by $g_1, \cdots, g_n$ is the homomorphic image of F_n, the free group on n generators. Thus the representation $g \to A_g$ of G restricted to G_n gives rise to a representation of F_n with bound M which, by hypothesis, is similar to a unitary representation via an operator P with $\| P \|$, $\| P^{-1} \|$ not exceeding $f(M)$. As in the proof of Theorem 1, we now conclude that $\| PA_{g_i}x_i \| = \| Px_i \|$, $i = 1, \cdots, n$; so that the representation is boundedly locally semi-simple with bounding constant $f(M)$. Hence, by Theorem 1, the representation $g \to A_g$ is similar to a unitary representation via a T such that $\| T \|$, $\| T^{-1} \|$ do not exceed $f(M)$. Thus B follows for all groups.

Note that the proof of Lemma 4 shows that assuming A for the class of groups generated by no more than a countable number of elements implies B for this class (since the group G constructed in the proof would be in this class). Now every group in this class is the homomorphic image of the free group on countably many generators, F_∞, so that assuming A for F_∞ implies A for all groups with a countable number of generators and hence B for the free groups on finitely many generators. With the theorem just proved, this yields:

COROLLARY 6. *If* A *holds for the free group on a countable infinity of generators then* A *and hence* B *holds for all groups.*

We turn our attention now to the question of topological semi-simplicity of algebras of operators. In Theorem 8, we state a necessary and sufficient condition for a representation of a C^*-algebra to be similar to a * representation. Before stating this result, however, it is necessary to introduce some geometrical concepts. In particular we must associate to each configuration of vectors an object which measures its deviation from being an orthonormal

set. To this end, we introduce an "inner product" between two sets of n vectors in $\mathcal{H}$. This inner product has as its range of values, operators on $\mathcal{H}$.

DEFINITION 2. *If $\tilde{x} = (x_1, \cdots, x_n)$, $\tilde{y} = (y_1, \cdots, y_n)$ are two n-tuples of vectors in $\mathcal{H}$ with $\mathcal{V}$, $\mathcal{W}$ the spaces generated by $\{x_1, \cdots, x_n\}$; $\{y_1, \cdots, y_n\}$, respectively, we denote by $\langle \tilde{x}, \tilde{y} \rangle$ the operator on $\mathcal{H}$ defined as follows. Let C^n be the space of n-tuples of complex numbers with the usual inner product and let $e_1, \cdots, e_n$ be the basis $(1, 0, \cdots, 0), \cdots, (0, \cdots, 0, 1)$. Let P be the map of C^n into $\mathcal{V}$ determined by $P(e_i) = x_i$, $i = 1, \cdots, n$, and let Q be the map of C^n into $\mathcal{W}$ determined by $Q(e_i) = y_i$. By Q^* we mean the adjoint map to Q, from $\mathcal{H}$ into C^n (characterized by $(Q^*x, a) = (x, Qa)$, where x is an arbitrary vector in $\mathcal{H}$, a in C^n, the first inner product is taken in C^n, and the second in $\mathcal{H}$). Then $\langle \tilde{x}, \tilde{y} \rangle = PQ^*$.*

We note some of the properties of $\langle\ ,\ \rangle$. As a function on the product of $\mathcal{H}_n$ (the n-fold direct sum of $\mathcal{H}$ with itself) with $\mathcal{H}_n$, this inner product is conjugate bilinear. Indeed with $\tilde{x} = (x_1, \cdots, x_n)$, $\tilde{x}' = (x_1', \cdots, x_n')$, $\tilde{y} = (y_1, \cdots, y_n)$, $\tilde{y}' = (y_1', \cdots, y_n')$, and $\langle \tilde{x}, \tilde{y} \rangle = PQ^*$, $\langle \tilde{x}', \tilde{y} \rangle = P'Q^*$, $\langle \tilde{x}, \tilde{y}' \rangle = PQ'^*$ we have

$$\langle \tilde{x} + \tilde{x}', \alpha\tilde{y} \rangle = (P + P')(\alpha Q)^* = \bar{\alpha}(PQ^* + P'Q^*) = \bar{\alpha}(\langle \tilde{x}, \tilde{y} \rangle + \langle \tilde{x}', \tilde{y} \rangle)$$

and similarly

$$\langle \alpha\tilde{x}, \tilde{y} + \tilde{y}' \rangle = \alpha(\langle \tilde{x}, \tilde{y} \rangle + \langle \tilde{x}, \tilde{y}' \rangle), \qquad \langle \tilde{x}, \tilde{y} \rangle = PQ^* = (QP^*)^* = \langle \tilde{y}, \tilde{x} \rangle^*.$$

With the notation as in the definition, we see that the range of $\langle \tilde{x}, \tilde{y} \rangle$ is contained $\mathcal{V}$ and that the range of $\langle \tilde{x}, \tilde{y} \rangle^* = \langle \tilde{y}, \tilde{x} \rangle = QP^*$ is contained in $\mathcal{W}$. Since the null space of an operator is the complement of the range of its adjoint, we have that the complement of $\mathcal{W}$ in $\mathcal{H}$ is the null space of $\langle \tilde{x}, \tilde{y} \rangle$. Thus, effectively, $\langle \tilde{x}, \tilde{y} \rangle$ is a transformation from $\mathcal{W}$ to $\mathcal{V}$.

We compute the transformation $\langle \tilde{x}, \tilde{y} \rangle$ precisely. With the notation above we have, for z in $\mathcal{H}$:

$$(Q^*z, e_i) = (z, Qe_i) = (z, y_i),$$

so that $Q^*z = \sum_{i=1}^{n} (z, y_i)e_i$, hence $PQ^*z = \sum_{i=1}^{n} (z, y_i)x_i$. Thus $\langle \tilde{x}, \tilde{y} \rangle$ can be expressed symbolically as $(\ , y_1)x_1 + \cdots + (\ , y_n)x_n$. It is immediate from this, that $\langle \tilde{x}, \tilde{x} \rangle$ is a positive operator on $\mathcal{H}$ (as it is from the expression PP^* for $\langle \tilde{x}, \tilde{x} \rangle$), and as such has a (unique) positive square root. We denote this square root by $\langle \tilde{x} \rangle$ and refer to it as "the geometrical norm of $\tilde{x}$ (or of the configuration $x_1, \cdots, x_n$)." The fact that $\langle \tilde{x} \rangle$ is the identity operator

on the n-dimensional space $\mathcal{V}$ (so that $x_1, \cdots, x_n$ are linearly independent, in particular) is equivalent to

$$\langle \tilde{x} \rangle^2 = \langle \tilde{x}, \tilde{x} \rangle = (\ , x_1)x_1 + \cdots + (\ , x_n)x_n$$

being the identity transformation on $\mathcal{V}$, which is equivalent to $x_1, \cdots, x_n$ being an orthonormal frame. The spread of the spectrum of $\langle \tilde{x} \rangle$, in general, is a measure of how much $x_1, \cdots, x_n$ deviates from being a scalar multiple of an orthonormal set. In the one-dimensional case, i.e., with x, y vectors in $\mathcal{H}$, we have $\langle x, y \rangle = (\ , y)x$. If we restrict this operator to the one-dimensional space generated by x, it becomes multiplication by (x, y), the usual inner product of x and y.

Suppose, now, that $\mathfrak{A}$ is a C^*-algebra and ϕ is a representation (not necessarily * preserving) of $\mathfrak{A}$ by operators on a Hilbert space $\mathcal{H}$. Employing Theorem 1, we obtain the following criterion for ϕ to be similar to a * representation.

THEOREM 7. *If $\mathcal{U}$ is the unitary group of the C^*-algebra $\mathfrak{A}$, a necessary and sufficient condition for a representation ϕ of $\mathfrak{A}$ by operators on a Hilbert space $\mathcal{H}$ to be similar to a * representation of $\mathfrak{A}$ is that ϕ restricted to $\mathcal{U}$ be a boundedly, locally semi-simple group representation of $\mathcal{U}$.*

Proof. If ϕ is similar to a * representation there exists an operator P on $\mathcal{H}$ such that $P^{-1}\phi(U)P$ is unitary, for each U in $\mathcal{U}$. Thus ϕ restricted to $\mathcal{U}$ is similar to a unitary representation of $\mathcal{U}$; and ϕ is boundedly, locally semi-simple, by Theorem 1. On the other hand, if ϕ is boundedly, locally semi-simple as a representation of $\mathcal{U}$ then, by Theorem 1, there exists an operator P on $\mathcal{H}$ such that $P^{-1}(U)P$ is unitary for each unitary operator U in $\mathfrak{A}$. It now follows that $A \to P^{-1}\phi(A)P$ is a * representation of $\mathfrak{A}$. Indeed, the given map is an algebraic isomorphism of $\mathfrak{A}$. Suppose A is a self-adjoint operator in $\mathfrak{A}$ of norm not exceeding 1. Then $A = \frac{1}{2}(U_1 + U_2)$ where $U_1 = A + i(I - A^2)^{\frac{1}{2}}$ and $U_2 = A - i(I - A^2)^{\frac{1}{2}}$ are unitary operators in $\mathfrak{A}$. Thus $P^{-1}\phi(A)P = \frac{1}{2}[P^{-1}\phi(U_1)P + P^{-1}\phi(U_2)P]$ with $P^{-1}\phi(U_1)P$ and $P^{-1}\phi(U_2)P$ unitary, so that

$$[P^{-1}\phi(U_i)P]^* = [P^{-1}\phi(U_i)P]^{-1} = P^{-1}\phi(U_i^{-1})P = P^{-1}\phi(U_i^*)P; \quad i = 1, 2.$$

Thus

$$[P^{-1}\phi(A)P]^* = P^{-1}\phi(\tfrac{1}{2}(U_1^* + U_2^*))P = P^{-1}\phi(A^*)P = P^{-1}\phi(A)P,$$

so that $A \to P^{-1}\phi(A)P$ takes self-adjoint operators in $\mathfrak{A}$ into self-adjoint operators, and, therefore, is a * representation of $\mathfrak{A}$.

Making use of the foregoing concept of inner product between sets of

n vectors, it is possible to give a more delicate analysis to the question of which representations of C^*-algebras are similar to * representations. If ϕ is a representation of a C^*-algebra $\mathfrak{A}$ by operators on a Hilbert space $\mathfrak{H}'$ ($\mathfrak{A}$ acts on $\mathfrak{H}$) and $\phi(A)x' = 0$ for some unit vector x' in $\mathfrak{H}'$, then for each positive ϵ one can find a unit vector x in $\mathfrak{H}$ such that $\| Ax \| < \epsilon$. Indeed, if $\phi(A_i)x' = 0$, $i = 1, \cdots, n$ one can choose the unit vector x so that $\| A_i x \| < \epsilon$, $i = 1, \cdots, n$, i. e., the relations $\phi(A_i)x' = 0$ can be "approximately duplicated" with $\mathfrak{A}$ and $\mathfrak{H}$ via ϕ. In fact, the set of operators A such that $\phi(A)x' = 0$ forms a proper left ideal $\mathfrak{J}$ in $\mathfrak{A}$ (proper, since $\phi(I) = I$). If for each unit vector x in $\mathfrak{H}$ one of $A_i x$ has norm not less than ϵ then $T = \sum A_i^* A_i \geqq \epsilon I$. But T is then invertible and in $\mathfrak{J}$. This contradiction implies the existence of the desired unit vector x. Given $\epsilon > 0$, vectors $x_1', \cdots, x_n'$ in $\mathfrak{H}'$ such that $\sum \| x_i' \|^2 = 1$, and relations $\sum_{i=1}^{n} \phi(A_{hi})x_i' = 0$, $h = 1, \cdots, m$; it is even possible to find vectors $x_1, \cdots, x_n$ in $\mathfrak{H}$ with $\sum \| x_i \|^2 = 1$ such that $\| \sum_{i=1}^{n} A_{hi}x_i \| < \epsilon$, $h = 1, \cdots, m$. This can be done by working with the $n \times n$ matrix algebras over $\mathfrak{A}$ and $\phi(\mathfrak{A})$ as we did above with $\mathfrak{A}$ and $\phi(\mathfrak{A})$ themselves. On the other hand, suppose the relations $\sum_{i=1}^{n} \phi(A_{hi})x_i' = 0$, $h = 1, \cdots, m$, subsist with $x_1', \cdots, x_n'$ an orthonormal set in $\mathfrak{H}'$; is it possible to choose $x_1, \cdots, x_n$ an orthonormal set in $\mathfrak{H}$ such that $\| \sum_{i=1}^{n} A_{hi}x_i \| < \epsilon$, $h = 1, \cdots, m$? This is not necessarily possible on two grounds; a multiplicity consideration, or more simply, the dimension of $\mathfrak{H}$ may not be large enough to accommodate an orthonormal set with n vectors, secondly, it is too much to ask for orthonormality of $x_1, \cdots, x_n$ in light of the fact that ϕ may not be a * representation (Theorem 8 shows that if it is possible to choose $x_1, \cdots, x_n$ an orthonormal set then ϕ is already a * representation). The multiplicity question can be avoided by asking whether or not a * representation ψ of $\mathfrak{A}$ can be found (once the relations $\sum_{i=1}^{n} \phi(A_{hi})x_i' = 0$ and $\epsilon > 0$ are given) such that $\| \sum_{i=1}^{n} \psi(A_{hi})x_i \| < \epsilon$. As for the orthonormality question, can we at least find bounds, dependent upon the representation ϕ alone, for the distortion of $x_1, \cdots, x_n$ from being an orthonormal set? The technique for measuring this distortion has just been developed. It is not difficult to see that if ϕ is similar to a * representation ψ via an operator P, then ψ will serve for the exact duplication of all relations with the distortion bounded by $\max(\| P \|, \| P^{-1} \|)$ (this will be done in detail in the necessity portion of Theorem 8). These considerations lead us to:

DEFINITION 3. *Let ϕ be a representation of the C*-algebra $\mathfrak{A}$ by operators on the Hilbert space $\mathfrak{H}$, and let $\tilde{x} = (x_1, \cdots, x_n)$ be an n-tuple consisting of vectors $x_1, \cdots, x_n$ which form an orthonormal set in $\mathfrak{H}$ such that $(\phi(A_{ij}))\tilde{x} = 0$, where $(\phi(A_{ij}))$ is an $n \times n$ matrix whose entries are operators in $\phi(\mathfrak{A})$. Let ψ be a * representation of $\mathfrak{A}$ by operators on a Hilbert space $\mathfrak{H}'$, and let $\tilde{x}' = (x_1', \cdots, x_n')$ be an n-tuple of vectors in $\mathfrak{H}'$ such that $\| (\psi(A_{ij})\tilde{x}' \| < \epsilon$, where ϵ is some positive number and the spectrum of $\langle \tilde{x}' \rangle$, as an operator on the space generated by $x_1', \cdots, x_n'$, is contained in the interval $[k, K]$. We say, then, that "$\| (\psi(A_{ij}))\tilde{x}' \| < \epsilon$ is a self-adjoint ϵ cover of the relations $(\phi(A_{ij}))\tilde{x} = 0$ with distortion in $[k, K]$." If there exist constants k, K, $(K > k > 0)$ such that each relation of the form $(\phi(A_{ij}))\tilde{x} = 0$, with $\tilde{x}$ as above and (A_{ij}) a positive operator (in the C*-algebra consisting of $n \times n$ matrices over $\mathfrak{A}$), has, for each positive ϵ, a self-adjoint ϵ cover with distortion in $[k, K]$, we say that "the representation ϕ has a self-adjoint cover (with distortion in $[k, K]$)."*

We have not made the definition of a representation having a self-adjoint cover as restrictive as we might, in that we require only relations coming from positive $n \times n$ matrices to have self-adjoint ϵ covers. This is all that is needed for each relation to have a cover. It might seem more natural to use the phrase "ϕ has a self-adjoint cover" to mean that for each ϵ there is a self-adjoint representation which serves as a self-adjoint ϵ cover of ϕ for all relations. That this actually follows from the weaker condition used and, indeed, that there is a self-adjoint representation which works for all positive ϵ and all relations is the substance of:

THEOREM 8. *A necessary and sufficient condition for a representation ϕ of a C*-algebra $\mathfrak{A}$ by operators on a Hilbert space $\mathfrak{H}$ to be similar to a * representation is that ϕ have a self-adjoint cover. If the distortion is in $[k, K]$ then a similarity can be effected by a positive operator with spectrum in $[k, K]$.*

Proof. The necessity presents little difficulty. Suppose that there exists an invertible operator T on $\mathfrak{H}$ such that $A \to T\phi(A)T^{-1}$ is a * representation of $\mathfrak{A}$, and let $M = \max(\| T \|, \| T^{-1} \|)$. If $(\phi(A_{ij}))\tilde{x} = 0$ is some relation, with $\tilde{x} = (x_1, \cdots, x_n)$, $x_1, \cdots, x_n$ an orthonormal set, then $(T\phi(A_{ij})T^{-1})\tilde{x}' = 0$ is a self-adjoint ϵ cover for this relation (all $\epsilon > 0$), where $\tilde{x}' = (Tx_1, \cdots, Tx_n)$, and where the distortion lies in $[1/M, M]$. Indeed, that $(T\phi(A_{ij})T^{-1})\tilde{x}' = 0$ with the given $\tilde{x}'$ is immediate. Let P be the linear transformation from C^n

into $\mathcal{H}$ defined by $Pe_i = x_i$ (see Definition 2), and let E be the projection on the space generated by $x_1, \cdots, x_n$. Then

$$\langle \tilde{x}', \tilde{x}' \rangle = TPP^*T^* = TET^* = (TE)(TE)^*.$$

Thus $\| \langle \tilde{x}', \tilde{x}' \rangle \| = \| TE \|^2 \leqq \| T \|^2 \leqq M^2$. Moreover

$$\begin{aligned}\inf\{(\langle \tilde{x}', \tilde{x}' \rangle x, x) : \| x \| = 1, x \text{ in } TE\mathcal{H}\} &= \inf\{\| (TE)^* x \|^2\} \\ &= \inf\{\| ET^*Ty \|^2 : y \text{ in } E\mathcal{H}, \| Ty \| = 1\} \geqq \inf\{(T^*Ty, y/\| y \|)^2\} \\ &= \inf\{\| Ty \|^4/\| y \|^2\} = \inf\{1/\| y \|^2 : y \text{ in } E\mathcal{H}, \| Ty \| = 1\} \geqq 1/M^2.\end{aligned}$$

Thus the spectrum of $\langle \tilde{x}', \tilde{x}' \rangle$ as an operator on $TE\mathcal{H}$ lies in $[1/M^2, M^2]$ so that the spectrum of $\langle \tilde{x}' \rangle$ lies in $[1/M, M]$, and $(T\phi(A_{ij})T^{-1})\tilde{x}' = 0$ is a self-adjoint ϵ cover (all $\epsilon > 0$) for $(\phi(A_{ij}))\tilde{x} = 0$ with distortion in $[1/M, M]$. In connection with foregoing inequalities, note that y is in $E\mathcal{H}$ so that the length of the projection of T^*Ty upon $E\mathcal{H}$ is not less than the length of the projection of T^*Ty upon the subspace generated by y (this length being $(T^*Ty, y/\| y \|)$).

Suppose now that the map ϕ has a self-adjoint cover. As in Theorem 1, we show that each finite-dimensional subspace $\mathcal{V}$ of $\mathcal{H}$ admits a Hilbert space norm $\| \ \|'$ such that $\| \phi(U)x \|' = \| \phi(V)x \|'$ when U, V are unitary operators in $\mathfrak{A}$ with $\phi(U)x, \phi(V)x$ in $\mathcal{V}$, and such that $k \| y \| \leqq \| y \|' \leqq K \| y \|$ for each y in $\mathcal{V}$. Following Theorem 1, form the conjugate tensor product $\mathcal{V} \otimes \mathcal{V}$ of $\mathcal{V}$ with itself and endow it with the unitary structure described in that theorem. Let $\mathcal{V}\otimes$ be the subspace of $\mathcal{V} \otimes \mathcal{V}$ generated by tensors of the form $x \otimes x$ and $\mathcal{E}\otimes$ the subspace generated by elements $\phi(U)x \otimes \phi(U)x - x \otimes x$, where U is a unitary operator in $\mathfrak{A}$ and $x, \phi(U)x$ are in $\mathcal{V}$. Choose a basis $\phi(U_1)y_1 \otimes \phi(U_1)y_1 - y_1 \otimes y_1, \cdots, \phi(U_m)y_m \otimes \phi(U_m)y_m - y_m \otimes y_m$ for $\mathcal{E}\otimes$ and an orthonormal basis $x_1, \cdots, x_n$ for $\mathcal{V}$. We have

$$\phi(U_i)y_i = \sum_{j=1}^{n} \beta'_{ij}x_j \text{ and } y_i = \sum_{j=1}^{n} \beta_{ij}x_j; \qquad i = 1, \cdots, m,$$

so that

$$0 = \sum_{j=1}^{n} (\beta_{ij}\phi(U_i) - \beta'_{ij})x_j = \sum_{j=1}^{n} \phi(\beta_{ij}U_i - \beta'_{ij}I)x_j; \qquad i = 1, \cdots, m.$$

Let a positive integer r and a positive number δ be given. We wish to establish the existence of a * representation ψ of $\mathfrak{A}$ as operators on a Hilbert space $\mathcal{H}'$ and vectors $x_1', \cdots, x_n'$ in $\mathcal{H}'$ such that $\langle \tilde{x}' \rangle$ has its spectrum in $[k, K]$, with $\tilde{x}' = (x_1', \cdots, x_n')$, and such that

$$\| \sum_{j=1}^{n} \psi(\beta_{ij}U_i - \beta'_{ij}I)x_j' \| < \delta; \qquad i = 1, \cdots, m.$$

We write A_{hj} for $\beta_{hj}U_h - \beta'_{hj}I$; $h = 1, \cdots, m$ and $\phi(A)^{\sim}$ for the $n \times n$ matrix whose i, j entry is the operator $\sum_{h=1}^{m} \phi(A_{hi}^*)\phi(A_{hj})$. Now $\phi(A)^{\sim}\tilde{x} = 0$, where $\tilde{x} = (x_1, \cdots, x_n)$, for

$$\phi(A)^{\sim} = \sum_{h=1}^{m} \begin{bmatrix} \phi(A_{h1}^*) & 0 \cdots 0 \\ \cdot & \cdot \quad \cdot \\ \cdot & \cdot \quad \cdot \\ \cdot & \cdot \quad \cdot \\ \phi(A_{hn}^*) & 0 \cdots 0 \end{bmatrix} \cdot \begin{bmatrix} \phi(A_{h1}) \cdots \phi(A_{hn}) \\ 0 \quad \cdots \quad 0 \\ \cdot \qquad \cdot \\ \cdot \qquad \cdot \\ \cdot \qquad \cdot \\ 0 \quad \cdots \quad 0 \end{bmatrix}$$

and

$$\begin{bmatrix} \phi(A_{h1}) \cdots \phi(A_{hn}) \\ 0 \quad \cdots \quad 0 \\ \cdot \qquad \cdot \\ \cdot \qquad \cdot \\ \cdot \qquad \cdot \\ 0 \quad \cdots \quad 0 \end{bmatrix} \tilde{x} = 0,$$

$h = 1, \cdots, m$. By hypothesis on ϕ, the relation $\phi(A)^{\sim}\tilde{x} = 0$ has a self-adjoint δ cover with distortion in $[k, K]$. Let ψ be a representation of $\mathfrak{A}$ by operators on the Hilbert space $\mathcal{H}'$ and let $\tilde{x}' = (x_1', \cdots, x_n')$ be a vector such that $\langle \tilde{x}' \rangle$ has spectrum in $[k, K]$ and $\| \psi(A)^{\sim}\tilde{x}' \| < \delta^2/n^{\frac{1}{2}}K$ where $\psi(A)^{\sim}$ is the $n \times n$ matrix whose i, j entry is $\sum_{h=1}^{m} \psi(A_{hi}^*)\psi(A_{hi})$. In particular then,

$$(\psi(A)^{\sim}\tilde{x}', \tilde{x}') \leqq \| \psi(A)^{\sim}\tilde{x}' \| \cdot \| \tilde{x}' \| < \delta^2$$

for

$$\| \tilde{x}' \| = (\sum_{i=1}^{n} \| x_i' \|^2)^{\frac{1}{2}} \leqq (\sum_{i=1}^{n} K^2)^{\frac{1}{2}} = n^{\frac{1}{2}}K.$$

In fact, since $\langle \tilde{x}' \rangle$ has spectrum in $[k, K]$, $\langle \tilde{x}', \tilde{x}' \rangle = \langle \tilde{x}' \rangle^2$ has spectrum in $[k^2, K^2]$, so that

$$\| \langle \tilde{x}', \tilde{x}' \rangle \| = \| PP^* \| = \| P \|^2 \leqq K^2 \text{ and } \| x_i' \| = \| Pe_i \| \leqq K$$

(notation as in Definition 2). Now $(\psi(A)^{\sim}\tilde{x}', \tilde{x}') =$

$$\sum_{h=1}^{m} \Bigg(\begin{bmatrix} \psi(A_{h1}^*) & 0 \cdots 0 \\ \cdot & \cdot \quad \cdot \\ \cdot & \cdot \quad \cdot \\ \cdot & \cdot \quad \cdot \\ \psi(A_{hn}^*) & 0 \cdots 0 \end{bmatrix} \cdot \begin{bmatrix} \psi(A_{h1}) \cdots \psi(A_{hn}) \\ 0 \quad \cdots \quad 0 \\ \cdot \qquad \cdot \\ \cdot \qquad \cdot \\ \cdot \qquad \cdot \\ 0 \quad \cdots \quad 0 \end{bmatrix} \tilde{x}', \tilde{x}' \Bigg)$$

$$= \sum_{h=1}^{m} \Bigg\| \begin{bmatrix} \psi(A_{h1}) \cdots \psi(A_{hn}) \\ 0 \quad \cdots \quad 0 \\ \cdot \qquad \cdot \\ \cdot \qquad \cdot \\ \cdot \qquad \cdot \\ 0 \quad \cdots \quad 0 \end{bmatrix} \tilde{x}' \Bigg\|^2.$$

Thus $\| \sum_{j=1}^{n} \psi(A_{hj}) x_j' \| < \delta$; $h = 1, \cdots, m$. Let $\mathcal{V}'$ be the subspace of $\mathcal{H}'$ generated by $x_1', \cdots, x_n'$, and let $y_1', \cdots, y_n'$ be an orthonormal basis for $\mathcal{V}'$. Denote by S the linear transformation determined by $Sy_i' = x_i'$. We assert that $SS^* = \langle \tilde{x}', \tilde{x}' \rangle = \sum_{i=1}^{n} (\ , x_i') x_i'$. Indeed, $(S^* x_i', y_j') = (x_i', Sy_j') = (x_i', x_j')$, so that $S^* x_i' = \sum_{j=1}^{n} (x_i', x_j') y_j'$ and

$$SS^* x_i' = \sum_{j=1}^{n} (x_i', x_j') S y_j' = \sum_{j=1}^{n} (x_i', x_j') x_j' = \langle \tilde{x}', \tilde{x}' \rangle (x_i').$$

Thus, since $x_1', \cdots, x_n'$ span $\mathcal{V}'$, $SS^* = \langle \tilde{x}', \tilde{x}' \rangle$ as asserted. It follows that SS^* has its spectrum in $[k^2, K^2]$ from which, $S^{-1*} S^{-1}$ has its spectrum in $[1/K^2, 1/k^2]$, so that $\| S \| \leqq K$ and $\| S^{-1} \| \leqq 1/k$. Let $S^* y_j' = \sum_{i=1}^{n} \alpha_{ij} y_i'$, so that the matrix of the transformation S^* relative to orthonormal basis $\{y_i'\}$ is (α_{ij}). In $\mathcal{V}$ define $y_j'' = \sum_{i=1}^{n} \alpha_{ij} x_i$. We set up a unitary transformation between $\mathcal{V}$ and $\mathcal{V}'$ by means of the map $x_i \to y_i'$. Under this map, we see that $y_j'' \to S^* y_j'$, so that

$$\begin{aligned}
&|(\sum_{j=1}^{n} y_j'' \otimes y_j'', \phi(U_i) y_i \otimes \phi(U_i) y_i - y_i \otimes y_i)| \\
&\quad = |(\sum_{j=1}^{n} S^* y_j' \otimes S^* y_j', [\sum_{h=1}^{n} \beta_{ih}' y_h'] \otimes [\sum_{h=1}^{n} \beta_{ih}' y_h'] - [\sum_{h=1}^{n} \beta_{ih} y_h'] \otimes [\sum_{h=1}^{n} \beta_{ih} y_h'])| \\
&\quad = |\sum_{j=1}^{n} (S^* y_j', \sum_{h=1}^{n} \beta_{ih}' y_h') (\sum_{h=1}^{n} \beta_{ih}' y_h', S^* y_j') \\
&\qquad - \sum_{j=1}^{n} (S^* y_j', \sum_{h=1}^{n} \beta_{ih} y_h') (\sum_{h=1}^{n} \beta_{ih} y_h', S^* y_j')| \\
&\quad = |\sum_{j=1}^{n} \{ |(y_j', \sum_{h=1}^{n} \beta_{ih}' x_h')|^2 - |(y_j', \sum_{h=1}^{n} \beta_{ih} x_h')|^2 \}| \\
&\quad = |\| \sum_{h=1}^{n} \beta_{ih}' x_h' \|^2 - \| \sum_{h=1}^{n} \beta_{ih} x_h' \|^2| = |\| \sum_{h=1}^{n} \beta_{ih}' x_h' \|^2 - \| \psi(U_i) (\sum_{h=1}^{n} \beta_{ih} x_h') \|^2| \\
&\quad \leqq \| \sum_{h=1}^{n} (\psi(U_i) \beta_{ih} x_h' - \beta_{ih}' x_h') \| \cdot [\| \sum_{h=1}^{n} \beta_{ih}' x_h' \| + \| \sum_{h=1}^{n} \psi(U_i) \beta_{ih} x_h' \|] \\
&\qquad \leqq \| \sum_{h=1}^{n} \psi(A_{ih}) x_h' \| (2n\beta K) \leqq 2n\beta K \delta,
\end{aligned}$$

where $\beta = \max \{ |\beta_{ih}|, |\beta_{ih}'| ;\ i = 1, \cdots, m;\ h = 1, \cdots, n \}$.

In connection with the above inequality, note that we have proved that $\| x_i' \| \leqq K$, and that $\psi(U_i)$ is a unitary operator on $\mathcal{H}'$ since ψ is a * repre-

sentation (with $\psi(I) = I$). We now specify the choice of δ as $1/2n\beta K r$ (all the constants that appear in this choice were determined before the introduction of δ). Our inequality becomes then:

$$|(\sum_{j=1}^{n} y_j'' \otimes y_j'', \phi(U_i)y_i \otimes \phi(U_i)y_i - y_i \otimes y_i)| \leqq 1/r; \qquad i = 1, \cdots, m.$$

We write $y_j(r)$ for y_j'' to indicate the dependence of the y_j'' upon r. Observe that $y_j(r)$ lies in the sphere of radius K and outside the sphere of radius k, center at 0, in $\mathcal{V}$ since $y_j(r)$ is the image of S^*y_j' under our unitary map between $\mathcal{V}$ and $\mathcal{V}'$ (and $\| y_j' \| = 1$, $\| S^* \| \leqq K$, $\| S^{*-1} \| \leqq 1/k$). By compactness, one can choose a subsequence $\{r_h\}$ of r's such that $\lim_h y_j(r_h) = z_j$; $j = 1, \cdots, n$. Clearly

$$(\sum_{j=1}^{n} z_j \otimes z_j, \phi(U_i)y_i \otimes \phi(U_i)y_i - y_i \otimes y_i) = 0; \qquad i = 1, \cdots, m,$$

and the z_j lie between the spheres of radii k and K with center at 0 in $\mathcal{V}$. We consider the norm $\| \ \|'$ induced on $\mathcal{V}$ by means of the definition:

$$(\| x \|')^2 = (\sum_{j=1}^{n} z_j \otimes z_j, x \otimes x) = \sum_{j=1}^{n} |(z_j, x)|^2.$$

We have just proved that $\sum_{j=1}^{n} z_j \otimes z_j$ is orthogonal to $\mathcal{E} \otimes$ so that $\| \phi(U)y \|' = \| y \|'$ if both $\phi(U)y$ and y are in $\mathcal{V}$. Thus, if $\phi(U)y$ and $\phi(V)y = \phi(VU^*)\phi(U)y$ are in $\mathcal{V}$ then $\| \phi(U)y \|' = \| \phi(V)y \|'$. For x an arbitrary vector in $\mathcal{V}$, we have $(\| x \|')^2 =$

$$\lim_h (\sum_{j=1}^{n} y_j(r_h) \otimes y_j(r_h), x \otimes x) = \lim_h (\sum_{j=1}^{n} S_h^* y_j'(h) \otimes S_h^* y_j'(h), x'(h) \otimes x'(h))$$

$$= \lim_h \sum_{j=1}^{n} |(y_j'(h), S_h x'(h))|^2 = \lim_h \| S_h x'(h) \|^2,$$

where $y_j'(h)$ are the vectors corresponding to y_j' in the foregoing discussion (with r_h now replacing r) S_h is the S of that discussion and $x'(h)$ is the image of x under the unitary map between $\mathcal{V}$ and $\mathcal{V}_h'$ of the present discussion. Now

$$\lim_h \| S_h x'(h) \|^2 \leqq \lim_h K^2 \| x'(h) \|^2 = \lim_h K^2 \| x \|^2 = K^2 \| x \|^2,$$

$$\lim_h \| S_h x'(h) \|^2 \geqq \lim_h k^2 \| x'(h) \|^2 = \lim_h k^2 \| x \|^2 = k^2 \| x \|^2,$$

so that $k \| x \| \leqq \| x \|' \leqq K \| x \|$.

If we take as partition classes in $\mathfrak{H}$ the sets $\{\phi(U)x: U$ a unitary operator in $\mathfrak{A}\}$, we arive at a situation satisfying the hypotheses of Lemma 3, so that $\mathfrak{H}$ admits a Hilbert space norm in which $\phi(U)$ is unitary for U a unitary operator in $\mathfrak{A}$ (this norm equivalent to the original norm with constants k, K). Thus, as at the end of the proof of Theorem 1, we can find an operator P with $P^{-1}\phi(U)P$ unitary for each unitary operator U in $\mathfrak{A}$ and $\|P\|$, $\|P^{-1}\|$ do not exceed $\max(K, 1/k)$. It now follows, as in the proof of Theorem 7, that the representation $A \to P^{-1}\phi(A)P$ is a * representation of $\mathfrak{A}$. Writing the polar decomposition HU, U unitary, $H = (PP^*)^{\frac{1}{2}}$ for P, we have $A \to H^{-1}\phi(A)H$ is a * representation of $\mathfrak{A}$ with H positive and having spectrum in $[k, K]$.

3. Concluding remarks. The discussion preceding Theorem 8 and Definition 3, concerning the approximate duplication of relations draws very heavily upon the fact that the initial algebra is a C^*-algebra (in particular, is uniformly closed) for the fact that an invertible operator in the algebra has its inverse in the algebra. On the other hand, Definition 3 and Theorem 8 apply as they stand to self-adjoint (not necessarily closed) algebras (although they are not stated this way). It follows immediately from this that:

COROLLARY 9. *A representation of a group by bounded operators on a Hilbert space is similar to a unitary representation if and only if the extension of this representation to the (finite, translation) group algebra (acting on L_2 of the group) has a self-adjoint cover.*

Despite the applicability of Definition 3 and Theorem 8 to self-adjoint algebras which are not uniformly closed, it should not be felt that the general conjecture about operator algebras has application to the non-closed, self-adjoint algebras. That is, examples are easily constructed of algebras which are not similar to self-adjoint algebras but are algebraically isomorphic to non-closed, self-adjoint algebras (not the continuous image, of course). In fact, let $x_1, x_2, \cdots$ be a sequence of linearly independent unit vectors which tend (strongly) to x and which span the Hilbert space $\mathfrak{H}$. Let $\mathfrak{A}$ be the algebra of bounded operators A on $\mathfrak{H}$ which have the form $Ax_i = \alpha_i x_i$ for some sequence $\{\alpha_i\}$ of complex numbers, and let $\mathfrak{s}$ be the set of sequences which arise in this manner ($\mathfrak{s}$ contains all sequences which have only a finite number of non-zero terms). Let $y_1, y_2, \cdots$ be an orthonormal basis for $\mathfrak{H}$ and let $\mathfrak{A}'$ be the algebra of operators B of the form $By_i = \alpha_i y_i$ where $\{\alpha_i\}$ is in $\mathfrak{s}$. Then $\mathfrak{A}'$ is a self-adjoint algebra containing I, for $B^*y_i = \bar{\alpha}_i y_i$ and $\{\bar{\alpha}_i\}$ is in $\mathfrak{s}$ if and only if $\{\alpha_i\}$ is in $\mathfrak{s}$ (the x_i's being so chosen that the

transformation $\alpha_1 x_1 + \cdots + \alpha_n x_n \to \tilde{\alpha}_1 x_1 + \cdots + \tilde{\alpha}_n x_n$ is bounded). Moreover the map $A \to B$ of $\mathfrak{A}$ onto $\mathfrak{A}'$ where $Ax_i = \alpha_i x_i$ and $By_i = \alpha_i y_i$ is an algebraic isomorphism (which is continuous, since $\| A \| \geqq \sup_i | \alpha_i | = \| B \|$). For each invertible operator P and each operator A in $\mathfrak{A}$, the operator $P^{-1}AP$ has $P^{-1}x_i$ as eigenvectors and these converge to $P^{-1}x$. Now the algebra $\mathfrak{A}$ is commutative (as is $P^{-1}\mathfrak{A}P$) so that, if $P^{-1}\mathfrak{A}P$ is self-adjoint then $P^{-1}AP$ is normal for each A in $\mathfrak{A}$. Given $i \neq j$ we can easily find a sequence $\{\alpha_p\}$ in $\mathfrak{H}$ with $\alpha_i \neq \alpha_j$ (let $\alpha_i = 1$, $\alpha_p = 0$ for $p \neq i$). Let A be the operator in $\mathfrak{A}$ with sequence $\{\alpha_p\}$. If $P^{-1}AP$ is normal then $P^{-1}x_i$ and $P^{-1}x_j$ are orthogonal. Thus if $P^{-1}\mathfrak{A}P$ is self-adjoint it follows that $P^{-1}x_i$, $i = 1, 2, \cdots$ is a set of mutually orthogonal vectors, which we have just seen cannot be the case.

We commented briefly, in the introduction, on the topological difficulty present in the infinite-dimensional case concerning the geometrical interpretation of semi-simplicity. By making suitable corrections for this difficulty, one arrives at a geometrical condition which might suffice for an algebra of operators to be similar to a self-adjoint algebra of operators. The conjecture obtained is quite natural in that it corrects for all the immediately visible difficulties which occur in passing from the finite to the infinite-dimensional case. For the moment, we specifically avoid describing the topology in which the operator algebra in question is closed.

Let $\mathfrak{A}$ be an algebra of operators on a Hilbert space with the property that there exists a positive δ such that if $\mathcal{V}$ is a closed subspace (setwise) invariant under the operators of $\mathfrak{A}$ then there exists a complementary closed invariant subspace $\mathcal{W}$ (i.e., *$\mathcal{V} + \mathcal{W}$ is the whole space and $\mathcal{V} \cap \mathcal{W} = (0)$*) *which makes an angle greater than δ with $\mathcal{V}$. Is $\mathfrak{A}$ similar to a self-adjoint algebra?*

Note that since the angle between $\mathcal{W}$ and $\mathcal{V}$ is assumed to be positive their linear sum is closed. Let us assume that the answer to this question is yes (with any closure assumption on $\mathfrak{A}$) and that A is a bounded operator on the Hilbert space $\mathcal{H}$ with no closed invariant subspaces other than (0) and $\mathcal{H}$. Let $\mathfrak{A}$ be the (commutative) algebra generated by A and the identity operator (the closure taken in the appropriate topology). Since $\mathfrak{A}$ has no closed non-trivial invariant subspaces, the hypothesis is vacuously satisfied and there exists an operator P such that $P^{-1}\mathfrak{A}P$ is self-adjoint. Since $P^{-1}\mathfrak{A}P$ is commutative, it consists of normal operators. In particular $P^{-1}AP$ is normal and has an abundance of non-trivial, closed, invariant subspaces. If $\mathcal{V}$ is such a subspace then $P\mathcal{V}$ is non-trivial, closed and invariant under

A—a contradiction. Again, if $\mathfrak{A}$ is an irreducible algebra of operators then the hypothesis are trivially satisfied, and an affirmative answer to the question would imply that $\mathfrak{A}$ is similar to a self-adjoint algebra. Making use of this remark, we can answer the question in the uniformly closed case negatively. Our own approach to this counter-example rested upon producing a uniformly closed irreducible operator algebra containing an invertible operator whose inverse didn't lie in the operator algebra (note that this can't occur in an algebra which is similar to a C^*-algebra). A much more cogent device was suggested to us by I. Kaplansky. Using the completely continuous operators as a basic irreducible set of operators, build a closed operator algebra over it whose quotient by the completely continuous operators is a (finite-dimensional), non-semi-simple algebra. The larger algebra is not even the isomorphic image of a C^*-algebra, for a quotient algebra of a C^*-algebra is again a C^*-algebra [8] and therefore semi-simple. A concrete example is obtained by taking as our algebra the algebra generated by the completely continuous operators, the identity operator, and a nilpotent operator of index two (say a partial isometry between an infinite-dimensional subspace and its orthogonal complement).

In conclusion, we note the simple fact that a representation of a group by uniformly bounded operators each of which is normal is itself a unitary representation. In fact, an invertible normal operator all of whose powers form a set which is uniformly bounded in norm must have its spectrum on the unit circle and is therefore unitary.

Added in proof (June 1, 1955): In a recent note, (*Proceedings of the National Academy of Sciences,* vol. 41 (1955)) F. Mautner and L. Ehrenpreis announce that the group question has a negative answer, i.e., they produce a group and a bounded representation of it which is not similar to a unitary representation. Presumably, then, the "distortion continuity" condition of Theorem 8 cannot be removed. Restricting attention to relations involving n or fewer vectors, we can discuss representations satisfying an "n-distortion continuity" condition—the boundedness of a group representation (or continuity of a C^*-algebra representation) amounts to "1-distortion continuity." We feel that there are groups and representations of them which have n but not $n+1$ distortion continuity.

COLUMBIA UNIVERSITY.

BIBLIOGRAPHY.

[1] M. M. Day, "Means for the bounded functions and ergodicity of the bounded representations of semi-groups," *Transactions of the American Mathematical Society*, vol. 69 (1950), pp. 276-291.

[2] J. Dixmier, "Les moyennes invariantes dans les semi-groupes et leurs applications," *Acta Szeged*, vol. 12 (1950), pp. 213-227.

[3] F. J. Murray and J. von Neumann, "On rings of operators," *Annals of Mathematics*, vol. 37 (1936), pp. 116-229.

[4] B. Sz. Nagy, "On uniformly bounded linear transformations in Hilbert space," *Acta Szeged*, vol. 11 (1947), pp. 152-157.

[5] M. Nakamura and z. Takeda, "Group representations and Banach limits," *Tôhoku Mathematical Journal*, vol. 3 (1951), pp. 132-135.

[6] G. Mackey, *Commutative Banach algebras*, Mimeographed lecture notes, Harvard, 1952.

[7] F. Peter and H. Weyl, "Die Vollstandigkeit der primitiven Darstellungen einer geschlossenen kontinuierlichen Gruppe," *Mathematische Annalen*, vol. 97 (1927), pp. 737-755.

[8] I. Segal, "Two-sided ideals in operator algebras," *Annals of Mathematics*, vol. 50 (1949), pp. 856-865.